DEPARTMENT OF THE NAVY
NAVAL INFORMATION SYSTEMS
MANAGEMENT CENTER

NAVSO P-5239-16
SEPTEMBER 1995

RISK ASSESSMENT

GUIDEBOOK

MODULE 16

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

0515-LP-208-8290

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Command, Control and Ocean Surveillance Center
In-Service Engineering East Coast Division
Code 423
4600 Marriott Road
North Charleston, SC 29406-6504

Commercial (803) 974-5423
DSN 563-2030 x5420
E-mail: subscribe@infosec.nosc.mil

Electronic versions of this document may be downloaded via anonymous ftp from infosec.nosc.mil or //hhtp//infosec.nosc.mil/inf.html.

Stocked: Additional copies of NAVSO P-5239-16 can be obtained from the Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia, PA 18120-5099, through normal supply channels in accordance NAVSUP P600, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8290.

NAVSO P-5239-16
SEPTEMBER 1995

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
ARLINGTON, VA 22202-4311

FOREWORD

Navy Staff Office Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. It consists of a series of modules providing procedural, technical, administrative, and/or supplemental guidance for all information systems, whether business or tactical, used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module will focus on a distinct program element and describe a standard methodology for planning, implementing, and executing that element of the INFOSEC program within the Department of the Navy (DoN).

This module, "Risk Assessment Guidebook," assists the Information Systems Security Manager (ISSM) and staff with guidance and procedures that could be used to perform risk assessments based on common, definable system and/or network configurations. It identifies and separates systems and networks by operating characteristics, and provides sample risk assessment methodologies that could be used for each situation.

The guidance contained herein applies to all DoN Information Systems and networks and is effective upon receipt.

J.G. HEKMAN
Rear Admiral, SC, USN

TABLE OF CONTENTS

TABLE OF CONTENTS

1.0 INTRODUCTION

The Department of the Navy (DoN) establishes policies for the protection of Information Systems (IS), networks, and other computer resources. These policies require all DoN activities to implement a cost-effective activity Information Systems Security (INFOSEC) Program, whose purpose is to protect an IS against unauthorized (accidental or intentional) data disclosure, modification, destruction, and denial of service. This document sets forth recommended guidelines for developing a cost-effective risk assessment program in support of the INFOSEC. It establishes a step-by-step method to determine system containment level, information sensitivity and criticality, environmental factors, security requirements, threat factors, and residual risks.

Note: Containment Level, which is a function of physical and logical relationships among systems, is described in more detail in paragraph 2.3 and Figure 1 along with the relative risk of exporting problems to other systems.

1.1 Applicability and Scope

This *Risk Assessment Guidebook* applies only to classified General Service (GENSER) and/or Sensitive Unclassified Information Systems. It *does not* apply to information systems processing Special Compartmented Information (SCI), cryptographic, cryptologic, Special Access Program, Single Integrated Operations Plan - Extremely Sensitive Information (S10P-ESI) or North Atlantic Treaty Organization (NATO) information. Guidelines for assessing risk in those systems are under the purview of the respective responsible authorities.

This *Guidebook* will focus on identifying threats, vulnerabilities, and countermeasures for assessed sites and/or assets. Specifically, it provides the following:

- Procedures for performing a cost-effective risk assessment on stand-alone systems, Local Area Networks (LANs), Wide Area Networks (WANs), and integrated site ISs.

- A color code system to be used when quantifying risk levels, rather than simply assigning a "Pass" or "Fail" to each risk item (see Appendix A, Assessment Coding Scheme).

- Detailed Risk Assessment (RA) Checklists for each risk area (see Appendix B, Risk Assessment Checklists), tailored to the needs of the system or network being assessed.

- A summarized list of terms.

1.2 Objective

The objective of this *Risk Assessment Guidebook* is to provide a cost-effective method for analyzing system and/or network risk. The risk assessment methodology contained herein builds on published Operational Navy Instruction (OPNAVINST) 5239.1A and Naval Research Laboratory (NRL) Report 8897 themes, as well as recent DoD draft risk assessment guidance. Properly implemented, it can be used to identify a system or network's most critical residual risk. The *Guidebook* presents the reader a suggested method for evaluating and performing a risk assessment on groups of "standard" or similar configurations. Additionally, this method can be used to perform risk assessments on an entire site, subject to similarities of system configurations and functions. Further, it is geared toward the system as it operates (e.g., safeguards that are in place within the system itself). Though this risk assessment methodology addresses issues associated with typical fielded systems, such as administrative or research, a more rigorous approach is required for complex developmental systems. Although recommended as an efficient roadmap to risk determination, use of the *Guidebook* is not mandatory.

Note: This *Risk Assessment Guidebook* is a suggested guideline only and is not a directive in nature. Rather, it is a suggested method for reducing the enormous cost of preparing a risk assessment.

1.3 Relationship to Other Directives

This publication supports OPNAVINST 5239.1A, and NRL Report 8897 by expanding their risk assessment themes and directing assessment efforts toward threat targets (e.g., communications, software, and network) as a means for determining real system or network threats.

1.4 Terms

For an extensive generic list of Terms, Abbreviations, and Acronyms, the reader should refer to NAVSOPUB 5239-02. This list is generic.

Countermeasure	An action, device process, procedure, technique, or other measure that reduces the vulnerability of an information system. Examples of countermeasure products include encryption, routers, bridges, authentication cards, network security monitors, and antivirus software.
Threat	Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstances or event with the potential to cause harm to, information or an information system.

Vulnerability — Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, and internal controls) that could be exploited to violate system security policy.

2.0 RISK ASSESSMENT GUIDELINES

This document provides guidance on a cost-effective approach to performing risk assessments on systems or networks in common operating environments, with like architectures, and similar use.

Risk Assessment Process — A risk assessment addresses system or network risk over its life cycle. Risk is determined by assessing the threats to a system and its vulnerabilities to those threats. One can never reduce threats to zero, nor is there an invulnerable system. Each threat-vulnerability mix will result in some unmitigated risk. That *residual risk* is of keen interest to the Designated Approving Authority (DAA) as he or she decides whether the residual risk is acceptable while making an accreditation decision.

Periodic Updates — Risk assessments should be living documents that mirror the progress of a system or network throughout its life cycle. Department of Defense (DoD)/DoN directives will dictate maximum time periods between risk assessments, but major system changes can also dictate risk assessment updates. Unless otherwise directed, updates are still made every 3 years, or in those cases where such changes might be:

- Major system redesigns
- Change in processed data sensitivity level
- Operating system or network software change.

Areas Addressed — This *Guidebook* provides the user with a tool that can be used to identify vulnerabilities in the assessed system or network after taking into account its available security safeguards and countermeasures. To determine the required level of risk assessment analysis, the following areas will be addressed: Containment Levels, Information Sensitivity, and Access Control Levels.

2.1 Information System Security Components

Information System Security encompasses several protection components, all of which, in varying degrees, affect the way a system or network's overall security requirements will be met. Their prime objective is to ensure that access to specific system information and/or capabilities is restricted to properly registered users possessing the appropriate clearances and privileges. The following paragraphs describe those essential security components.

Confidentiality

Confidentiality reflects the protection given to data so that only authorized entities (users, processes, or "foreign" systems or networks) are allowed to access it in a controlled manner, and that unauthorized entities are barred from that access. The term "confidentiality" is used instead of "secrecy" to avoid unwarranted implications that this security component is solely the domain of the Government. All organizations, in or out of Government, have a requirement to protect certain information. Even owners of clearing house operations or electronic bulletin boards require the ability to prevent unwanted access to supervisory functions within their system. Confidentiality is at the heart of any INFOSEC policy. Threats to confidentiality, whether malicious or accidental, can result in unauthorized disclosure of sensitive system information.

Integrity

Integrity is perhaps the most complex and misunderstood security component. Integrity is an information systems security characteristic that ensures that computer resources operate correctly and that the data handled by the system are correct. This characteristic protects against deliberate or inadvertent unauthorized manipulation of the system or network and ensures the security of entities of a computer system under all conditions.

- **Data Integrity.** Data Integrity refers to that attribute of data relating to the preservation of the following:

  - Its meaning and completeness
  - The consistency of its representation(s)
  - Its correspondence to what it represents.

Data integrity is a matter of degree with regard to the quality of the information itself and not who does or does not have access to it. Integrity also relates to the quality of information and identifies
how closely the data corresponds to reality. Parallel questions

outside the information system community might be: How closely

does a resume reflect a person's real abilities? Does a credit report accurately reflect the individual's historical record of financial transactions? The definition of integrity implicitly includes the broad scope of accuracy, relevancy, and completeness to meet its protection roles. Thus, data integrity calls for a comprehensive set of aids to promote accuracy and completeness as well as security.

- **System Integrity.** Every system or network has a defined set of hardware, software, and operating parameter configurations. The intent of these preestablished configurations is to ensure that the system performs its intended function in an unimpaired manner. To do so, it must be free from deliberate or inadvertent unauthorized manipulation. System integrity defines the state that exists when there is complete assurance that under all conditions a system is based on the logical correctness and reliability of the operating system, the logical completeness of the hardware and software that implement the security protection mechanisms, and the configurable parameters under which that system or network will operate.

Availability

Availability describes an authorized user's ability to access a system or network's capabilities as required, without interruption. This vital aspect of security ensures system capabilities and information is provided to authorized users when it is requested or needed. Often it is viewed as a less technical requirement that is satisfied by redundancy within the information system such as back-up power, spare data channels, and parallel databases. Threats to availability also include unauthorized access to network management functions (e.g., reset and shutdown), resource monopolization (message flooding), and physical damage.

Accountability

Systems used to process or handle sensitive unclassified and or classified information must assure individual accountability whenever either a discretionary or mandatory security policy is invoked. That accountability must account for individuals, processes, and other systems accessing an information system.

Accountability has utility in two ways. First, as long as properly registered users access a system or network's capabilities and data
in accordance with that system's security policy, accountability provides an additional level of assurance that a user's data will be

properly handled and maintained. Second, where some user or process violates (intentionally or unintentionally) that system's security policy, it gives system Trusted Officials the ability to identify and rectify the situation. Trusted officials are system or network management officials with extraordinary system privileges who are trusted *not* to abuse those privileges.

2.2 Configuration

A system or network configuration defines the relationship of that entity to other systems or networks as well as the relationship between the components within the network. If a vulnerability exists in one, its risk to other connected entities must also be evaluated. Network topologies may be designed to handle one of two distinct needs, either wide area or local area communications. They may also include a requirement to intercommunicate on both the wide area and local area scales. Thus, this *Guidebook* will focus on specific local area, wide area, and integrated topologies with primary emphasis on conducting network risk assessments rather than multiple individual host assessments. The following configurations are noted for your reference during your system, network, or site assessments. (Future revisions of this pub will contain configurations with identified vulnerable areas that users should be aware of when setting up firewalls.)

Self-Contained System

A self-contained system provides its mission services without relying on network connections to other systems. It is functionally self-sufficient, and although it may have network connectivity or interface, it does not require that network service to satisfactorily accomplish its primary mission.

Wide Area Network (WAN)

Connecting multiple user computers, WAN technology is based on the need to communicate over wide geographic regions. These networks are characterized by relatively slow speeds, small bandwidth (information carrying capacity), tendencies to be relatively error prone, and multiple communications nodes. Most communications channels are provided by a third party, such as a commercial carrier, rather than being owned "in-

house." In many cases, packet switching has been chosen as the most economical and responsive method for such long-distance exchanges.

Local Area Network (LAN)	A LAN has a number of characteristics that distinguish it from a WAN. These include connecting computers over a much smaller geographic region (some even within a single room), throughput several orders of magnitude higher than a WAN, extremely short delay, and large total bandwidth. Most LANs are owned by the using organization, and exhibit a much lower error rate than WANs. The most common LAN topologies today include Ethernet, Token Ring, Token Bus, and Fiber Distributed Data Interface (FDDI). These network topologies directly support the client-server computing model, a model where specialized hosts (servers) provide common services to a wide variety of network participants (clients). Common server applications include file sharing, remote login, remote printing, and network name service. Note that a single server process must normally be able to concurrently support access requests from a distributed community of clients.
Integrated System	An integrated system is one that relies on distributed computing and communications assets to accomplish its primary mission. It may employ a wide range of host computers, workstations, servers, and network communications services to provide its users with the capabilities they require.

2.3 Containment Level

Containment Level is a concept for addressing the relative likelihood that a system security problem could migrate to and adversely affect other systems or networks. Containment Level, which is a function of physical and logical relationships among systems, is described in more detail in Figure 1 along with the relative risk of exporting problems to other systems.

System Type	Export Risk	System Description
Benign	Low	A system that is not related to any other system is a benign system. Benign systems are closed communities without physical connection or logical relationship to any other systems. Benign systems are operated exclusively of one another and do not share users, information, or end processing with other systems. An isolated (e.g., no network connection) personal computer (PC) limited to word processing, spreadsheet and/or database application functions is an example of a benign system.
Passive	Low to Moderate	A system that is related indirectly to other systems is passive. Passive systems may or may not have a physical connection to other systems, and their logical connection is controlled tightly. Stand-alone IS that pass information to other IS via magnetic media ("air gap") are passive. Systems that are physically connected but only receive information are passive. Although passive systems may use protocols to interact with other systems, they do not have interactive sessions with other systems; transmit information to other systems; or permit the extension of their users or processes by read, write, or execute privileges over any network shared with other systems. The following are examples of passive systems: • A series of non-networked PCs where data is passed among PCs for continued processing via diskette. • A meteorological system that relies on inputs from various sensor systems to generate local displays, weather forecasts, and the like. • A financial system where expenditure data is fed into the host system with no capability for those entering data to receive information from that host.
Active	Moderate to High	A system that communicates interactively with one or more other systems is active. Active systems are physically connected and have a logical relationship to other systems. Active systems may permit users and/or processes to access and modify multiple system resources. They allow users to alter data or provide limited restrictions to system resources. An active system may allow interactive sessions, process initiation, or user-defined queries across multiple systems. An example of an active system would be a client-server database system relying on networked assets (e.g., database host computer, applications servers, print servers, workstations, and the like) to perform its mission.

Figure 1. Containment Level

2.4 Computer Security Policy and Requirements Determination

IS security requirements stem from more generalized security requirements encompassing a wide range of protective countermeasure or safeguard elements. There are two very basic security policy options that any system or network may implement. Computer Security Policy options are as follows:

- Unless otherwise explicitly denied, grant access to system information and capabilities
- Unless otherwise explicitly granted, deny access to system information and capabilities.

From an information systems security viewpoint, the latter option, deny access unless explicitly granted, provides a more secure and controllable processing environment. Prior to defining its security requirements, a system or network must first have an established and documented security policy.

Establishing Policy

Security policy statements form the basis for required IS security protection features. There are three basic security policy sources: regulatory, operational, and criticality.

- **Regulatory.** Public Laws, Executive Orders (E.O.) and many federal and DoD regulations mandate certain security policies for all or selected ISs. For example, basic national security requirements include protecting sensitive data or information from compromise, service denial, or unauthorized alteration. Information sensitivity (for example, security classification) is the direct result of applying regulatory policies.

- **Operational.** Security policies are also influenced by operational requirements, such as system performance, necessary personnel clearances, budget constraints, and the operating environment. In consideration of these items, security policies sometimes make tradeoffs to evolve the best mix of security protection, performance, and cost.

- **Criticality.** A policy should also consider the system's criticality. Criticality is an indicator of the system's importance to the mission that it performs or supports. It considers national security, safety, human health factors, and the organizational level involved. Criticality introduces the operational mission into the security requirements equation,
and influences the combination of internal safeguards,

---

security operating mode, and other security protection features selected for the Information System.

Implementation

When implementing a security policy, consider both external and internal measures.

- **External Security Protection Measures.** Sometimes known as countermeasures, these security protection features exist outside the physical or logical boundaries of the IS. These security features include the physical, personnel, administrative, and procedural security discipline areas as well as Emanations Security (EMSEC, also called TEMPEST) and Communications Security (COMSEC).

- **Internal Security Protection Measures.** Sometimes known as safeguards, these security protection features exist inside the system's physical or logical boundaries. They focus on operating system-based security mechanisms, but there can be some overlap with other disciplines (e.g., the specialized engineering done for TEMPEST countermeasures). Internal security protection measures frequently begin with a Trusted Computing Base (TCB) equipped operating system.

2.5 Information Sensitivity

Each system or network's mission will, in large part, determine the sensitivity of the information it processes. That sensitivity in turn dictates the Information System's applicable security requirements. The information sensitivity level can be expressed in terms of classification, special access categories, and handling restrictions. Systems that process, transmit, or store information at more than one sensitivity level may be responsible for identifying, separating, and controlling that information by sensitivity level (as in *multilevel secure* systems). On a less rigorous scale, *Discretionary Access Control* systems may allow users to pass access privileges to other users for certain sensitive data. In any case, these systems must satisfy all security requirements associated with the most sensitive data processed by the system or network. Information sensitivity can be categorized as follows:

Classified National Security Information

E.O. 12958 establishes guidelines for classifying information deemed vital to the national security interests of the United States. Those classifications are *hierarchical*, in that one dominates the other. For example, a data file classified TOP SECRET may also include data or information classified SECRET, but the TOP SECRET classification dominates the lower one. Within the hierarchical classification structure, there are *nonhierarchical* information categories. To access one of those nonhierarchical categories, an individual must first possess the necessary hierarchical clearance; in addition, the individual must be granted special access to the nonhierarchical category. Finally, some classified information does not fit into a special access category, yet carries certain handling restrictions (e.g., NOFORN).

- **Nonhierarchical Categories.** Two examples of nonhierarchical classified information categories include SCI and SIOP-ESI. Usually used by the intelligence community, an individual is normally not granted SCI access until having received training for its special access and handling restrictions. SIOP-ESI is information contained in the nation's most secret war plans. That information is only accessible by those cleared for and indoctrinated into its critical handling and release requirements.

- **Handling Restrictions.** Classified information may also contain one or more of several handling restrictions. Handling restrictions usually do not employ separate and identifiable access control programs, but are guidelines for dissemination of that information. Two examples are *No Foreign Nationals (NOFORN) Dissemination*, where access should be denied foreign nationals, *Formerly Restricted Data*, relating to certain nuclear weapons design information.

Sensitive Unclassified Information

This category includes information not designated as classified National Security information, but having a sensitivity that would prevent its free and open public disclosure. Information covered by the Privacy Act, such as Social Security Numbers, as well as medical, pay, and personnel information fall into this category. Other information that might be designated Sensitive

	Unclassified Information is budget and financial data, proprietary contractual data (such as proposals and pricing information), information designated For Official Use Only, and information affecting safety and human life (such as air traffic control data).
Unclassified Information	This category includes all information that is free and open for distribution to the public, such as news releases and information on housekeeping activities.

2.6 Access Control Levels

Access control combines the sensitive information processing environment, known as the Security Operating Mode, with available external countermeasures and internal operating system security safeguards.

Security Operating Mode	A Security Operating Mode describes the sensitive information processing environment. Each security mode exhibits a different relationship between internally and externally provided security protection features. Figure 2 describes the several different security operating modes.

Dedicated Security Mode	All information that the system processes is considered classified at one level only. All users have the clearance and a need-to-know for all information handled by the system. There is a heavy reliance, normally exclusive reliance, on externally provided security protection features to prevent compromise, and little, if any, trust is placed in internal system safeguards.
System High Security Mode	All users are cleared to the highest level processed by the system or network, but do not necessarily have a need-to-know for all information handled by the system. There is a heavy reliance on externally provided security protection features, with some internally provided elementary discretionary controls
Multilevel Security Mode	The system identifies, separates, and controls information at different sensitivity levels. Likewise, the user community may have different clearances and need-to-know levels. Internal and external controls share the responsibility for protecting information. These controls apply in varying degrees, depending on the information's sensitivity and user's clearance.

Figure 2. Security Modes

Security Safeguard Features

Figure 3 illustrates the relative reliance placed on external (e.g., physical and procedural) and internal (e.g., computer access control mechanisms) measures to enforce a system or network's security policy.

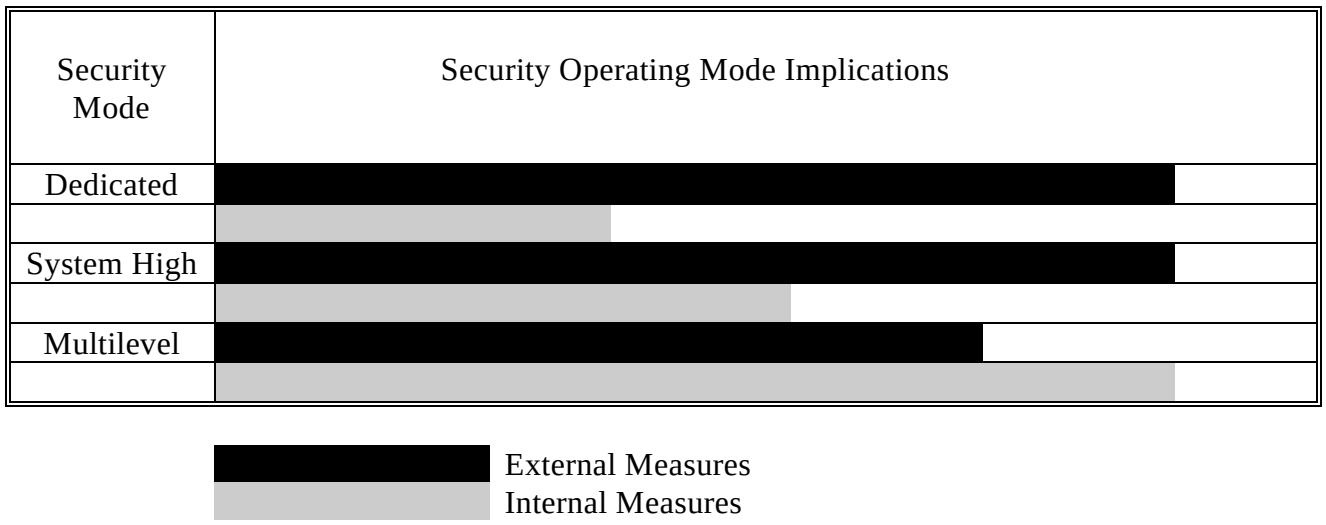

Figure 3. Security Operating Mode Implications

2.7 Network Risk Assessments

Network Risk Assessments present a particularly difficult challenge because of the many risk combinations and permutations that might exist. When performing network risk assessments, the network's various components should be analyzed and a "weakest link" philosophy should be employed toward overall network risk. Figure (4) and (5) graphic, portray a typical input(transmit)-process(transport)-output(receive) sequence.

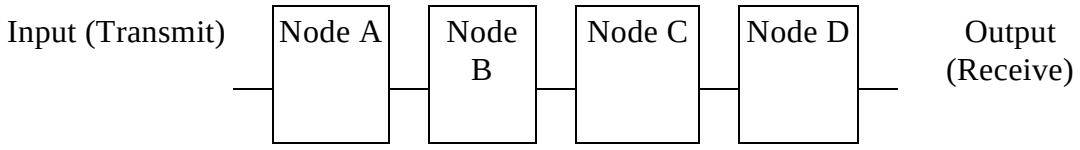

Figure 4. Input/Output Sequence

Consider the two sample cases that follow.

Case	Node	Security Operating Mode	Accredited Sensitivity Level
1	A	System High	Sensitive Unclassified
	B	Multilevel	Secret
	C	System High	Sensitive Unclassified
	D	Dedicated	Unclassified
2	A	Multilevel	Top Secret
	B	System High	Secret
	C	Multilevel	Top Secret
	D	Multilevel	Top Secret

Figure 5. Sample Cases

3.0 RISK ASSESSMENT PROCEDURES

To characterize the system or network being analyzed and determine the Risk Assessment type most appropriate, follow the steps below. Review Appendix A, Assessment Coding Scheme, to ensure that you understand the risk ranking factors used. Completing these steps will determine those sections of the Risk Assessment Checklists in Appendix B that apply to your assessment. During or after completing the appropriate checklist sections, determine your rating for each element within the "Assessed Areas."

This section and Appendix B are designed to be used as worksheets that can be included in the Accreditation Package. The Accreditation Package will be forward to the system or network DAA for accreditation decision. An optional alternative would be to include the Final Assessment Summary in lieu of the Risk Assessment Checklist.

3.1 Security Component Rank Order

Determine, in rank order, the IS Security Components most critical to your system or network (see paragraph 2.1 for details). This determination will be subjective on your part as to the relative importance between Confidentiality, Integrity, Availability, and Accountability. Record them in rank order here:

Criticality	Security Component	Remarks
Most Critical	Confidentiality Availability Integrity Accountability	
Second Most Critical	Confidentiality Availability Integrity Accountability	
Third Most Critical	Confidentiality Availability Integrity Accountability	
Least Critical	Confidentiality Availability Integrity Accountability	

Figure 6. Security Component Ranking Form

3.2 Configuration

Determine your system or network configuration (see paragraph 2.2 for details).

Configuration	(Self Contained)	(WAN)	(LAN)	(Integrated System)

Figure 7. Configuration Types

3.3 Containment Level

Determine the Containment Level that applies to your system or network (see paragraph 2.3 for details).

Containment Level	(Benign)	(Passive)	(Active)

Figure 8. Containment Level Types

3.4 System Security Policy

Review the system or network security policy(ies) for any specific security requirements applicable to your system or network (see paragraph 2.4 for details).

Specific Security Requirements	

Figure 9. Security Requirements

3.5 Information Sensitivity

Determine the maximum sensitivity level for information processed, stored, or transmitted by your system or network (see paragraph 2.5 for details).

Sensitivity Level	(Unclass) (Sens. Unclass) (Class) (Class w/ Handling Restr) (Class w/ Categories)

Figure 10. Information Sensitivity Types

3.6 Access Control Level

Determine your system or network's Access Control Level (Security Operating Mode) using the guidance contained in paragraph 2.6.

Access Control Level (Security Operating Mode)	(Dedicated)	(System High)	(Multilevel)

Figure 11. Access Control Level Types

3.7 Risk Assessment Type

This *Guidebook* presents four risk assessment types, based on a system's risk potential as described in the above paragraphs. Those assessment types and their intended uses are described below:

Survey Risk Assessment	The simplest and most straightforward, this risk assessment type is used only for systems operating in the Dedicated Security Mode and processing sensitive unclassified and/or classified information. The checklist items for this assessment confirm that physical, procedural, and personnel risks associated with the Dedicated Security Mode are within acceptable limits.
Basic Risk Assessment	This assessment type includes all items in a Survey Risk Assessment, and begins to look into logistics risk areas and system-enforced discretionary controls.
Intermediate Risk Assessment	This assessment type includes items in the previous assessment types, and extends the level of system safeguards and communications risk areas.
Full Risk Assessment	Reserved for the most complex systems and those with the highest information sensitivity, a full risk assessment requires completing all portions of the attached checklists (except for any illogical or inappropriate items) and any additional risk determination dictated by the system or network architecture, implementation method, or other extraordinary circumstance.

Use the chart below (Figure 12) to determine your risk assessment type. Read down the left most column until you find the containment description for your system. Follow along to the right selecting the path that describes your security operating mode. Continue along to the right selecting the appropriate description for the sensitivity level handled by your system. Finally, continuing along to the right, you will find the proper risk assessment for your system listed. Note that not all combinations of containment, security operating mode, and sensitivity level appear here. Many are illogical (e.g., active *and* dedicated), and others will be found only on rare occasions. You may need to consult paragraph 2.2, Configuration, and 2.7, Network Risk Assessments, before deciding the risk assessment type required for your system. If your containment-security operating mode-sensitivity level combination is not on this list, consult with your DAA or the DoN INFOSEC Personnel at NCCOSC In-Service Engineering East Coast Division (commercial (803) 974-5423) for guidance.

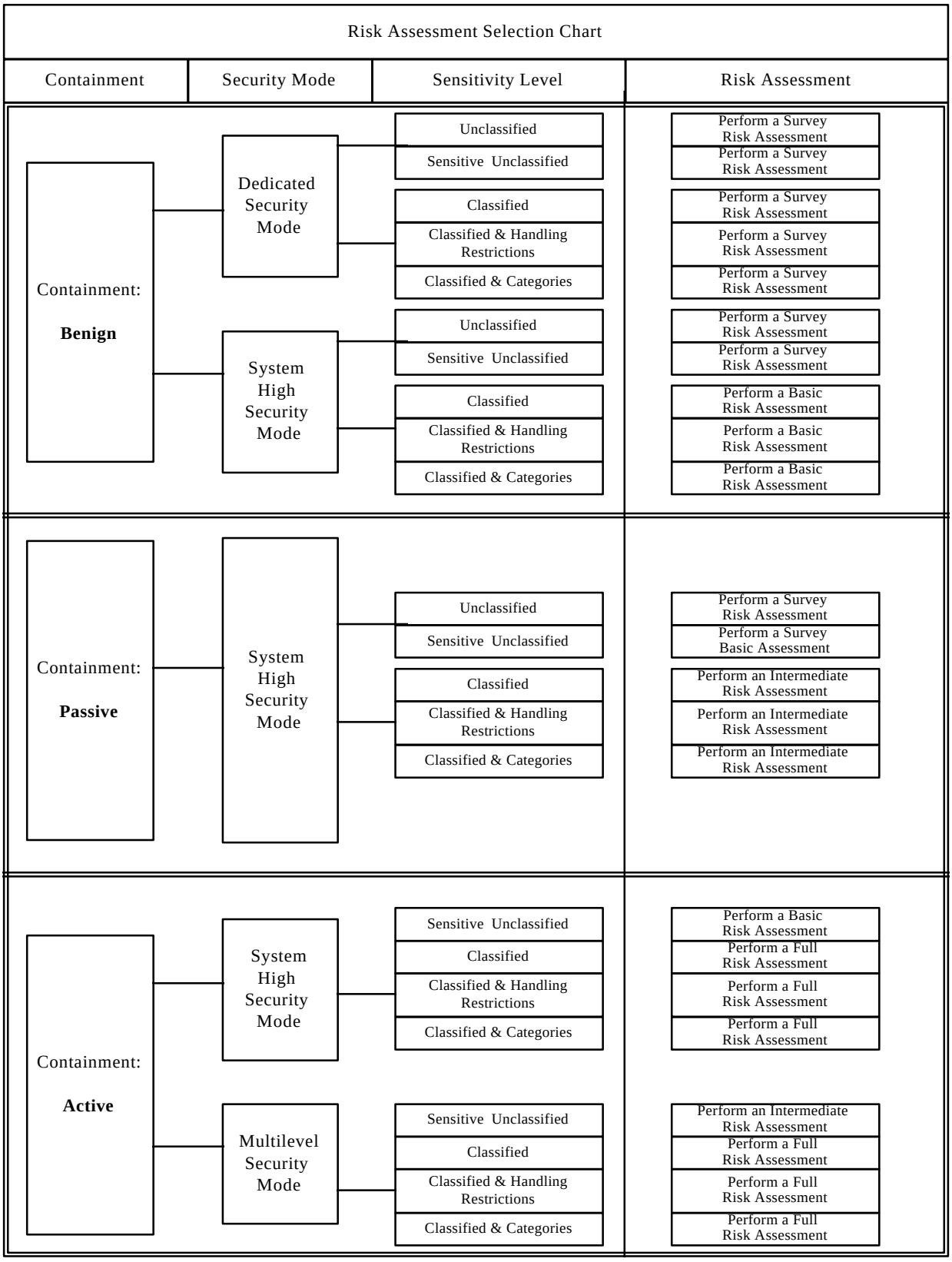

Figure 12. Risk Assessment Selection Chart

3.8 Complete Worksheets .

Consult the Risk Assessment Topic Selection Chart to determine which of the Risk Assessment Checklists contained in Appendix B apply to your Risk Assessment. Add any checklist items that might be needed because of unique system security policy requirements or other germane factors (e.g., criticality, operational mission, command and control systems, and complete site assessments). Document the most critical residual risk at the end of each assessed area in Appendix B (in Overall Summary at the end of Appendix B is optional), and include the results of this risk assessment in the Accreditation Package forwarded to the system or network DAA.

Risk Assessment Topic Selection Chart					
Assessment Area	Include in Risk Assessment Type				Remarks
	Survey	Basic	Interme d	Full	
1. Administrative Assessment Area					
• System Administrator's Manual	--	--	Yes	Yes	
• End User's Manual	Yes	Yes	Yes	Yes	
• Trusted Facility Manual	--	--	--	Yes	
• Standard Operating Procedures	Yes	Yes	Yes	Yes	
• Operational Consumables	Yes	Yes	Yes	Yes	
• *reserved*					
2. Communications Assessment Area					
• Circuit Identifiers	--	--	Yes	Yes	
• Site WAN (LAN)	--	--	Yes	Yes	
• Physical Protection	--	--	Yes	Yes	
• Operational Continuity	--	--	Yes	Yes	
• *reserved*					
3. Emanations Assessment					
• Installation Practices	--	Yes	Yes	Yes	
• TEMPEST Certifications	Yes	Yes	Yes	Yes	
• reserved					
4. Information Assessment Area					
• Responsible Security Official(s)	Yes	Yes	Yes	Yes	
• Information Sensitivity	Yes	Yes	Yes	Yes	

• Information Access Controls	Yes	Yes	Yes	Yes	
• Information Storage	Yes	Yes	Yes	Yes	

Risk Assessment Topic Selection Chart					
Assessment Area	Include in Risk Assessment Type				Remarks
	Survey	Basic	Interme d	Full	
• Information Handling	Yes	Yes	Yes	Yes	
• Information Destruction	Yes	Yes	Yes	Yes	
• *reserved*					
5. Logistics Assessment Area					
• Developmental Assurances	--	--	--	Yes	
• Operational Assurances	--	--	Yes	Yes	
• Life-cycle Assurances	--	_	Yes	Yes	
• Accreditation	Yes	Yes	Yes	Yes	
• *reserved*					
6. Network Assessment Area					
• Connectivity Services	--	--	Yes	Yes	
• Transport Services	--	--	Yes	Yes	
• Name Server Services	--	--	Yes	Yes	
• Internet Server Services	--	--	Yes	Yes	
• Terminal Server Services	--	--	Yes	Yes	
• Network Registration Services	--	--	Yes	Yes	
• Network I&A Services	--	--	Yes	Yes	
• Network Access Control Services	--	--	Yes	Yes	
• Network Auditing Services	--	--	--	Yes	
• Network Monitoring Services	--	--	--	Yes	
• Network Ops Security Services	--	--	--	Yes	
• *reserved*					

Risk Assessment Topic Selection Chart					
Assessment Area	Include in Risk Assessment Type				Remarks
	Survey	Basic	Intermed	Full	
7. Personnel Assessment Area					
• Functional Users	Yes	Yes	Yes	Yes	
• Functional User Group Members	--	Yes	Yes	Yes	
• Trusted Officials	--	Yes	Yes	Yes	
• Network Trusted Officials	--	--	Yes	Yes	
• *reserved*					
8. Physical Assessment Area					
• Facility	--	--	Yes	Yes	
• Operations Area	Yes	Yes	Yes	Yes	
• Communications Closet	Yes		Yes	Yes	
• Functional User Workplace	Yes	Yes	Yes	Yes	
• *reserved*					
9. Software Assessment Area					
• Registration Rule	--	Yes	Yes	Yes	
• Identification & Authentication Rule	--	Yes	Yes	Yes	
• Discretionary Access Control Rule	--	Yes	Yes	Yes	
• Mandatory Access Control Rule	--	--	Yes	Yes	
• Security Audit Trail Rule	--	Yes	Yes	Yes	
• Object Reuse Rule	--	--	--	Yes	
• Viruses	Yes	Yes	Yes	Yes	
• *reserved*					

Risk Assessment Topic Selection Chart					
Assessment Area	Include in Risk Assessment Type				Remarks
	Survey	Basic	Intermed	Full	
10. UNIX Network Security Model					
• Operating System	--	Yes	Yes	Yes	
• Auditing	--	Yes	Yes	Yes	
• Firewalls	--	--	Yes	Yes	
• Routers	--	--	Yes	Yes	
• *reserved*					

Figure 13. Risk Assessment Topic Selection Chart

APPENDIX A: ASSESSMENT CODING SCHEME

The "color code" approach below has been adopted to help discriminate the relative rank among risks. Although still somewhat subjective, this coding scheme allows more specificity than a simple "pass" or "fail" rating.

Assessment	Assessment Description	Assessed Risk Descriptor
Blue ("B")	Exceeds minimum standard for the risk area in a way that significantly enhances security. Example: Using data encryption to protect sensitive unclassified information during transit. Risk mitigation approach is superior to other potentially acceptable solutions.	Low risk; little to no action needed to reduce risk to system or data.
Green ("G")	Meets standards in a reasonable and responsible manner. Example: Cipher locks and entry control rosters for computer rooms. Risk mitigation approach is sound and equivalent to accepted practices.	Acceptable risk; risk can be reduced where needed using routine action.
Yellow ("Y")	Fails to meet minimum standard, but can be corrected. Example: No instructions to system administrators or users on secure system operation. Risk mitigation approach is inferior to accepted practices.	Moderate to high risk, depending on data sensitivity and mission criticality. System officials must take positive corrective action to reduce risk to an acceptable level.
Red ("R")	Fails to meet minimum standard in unacceptable ways. Example: Uncontrolled access to UNIX root prompt. Risk mitigation approach is significantly flawed and requires correction.	Unacceptably high risk; extraordinary action required to mitigate before the system is placed on-line for operational use.

Assessment coding scheme further clarified: An overall rating should be applied to each assessment area. This overall rating is subject to the evaluator's discretion. Deciding an overall rating is subjective; the evaluator would be making a judgment call based on the threat to the system being analyzed. An example of how to decide an overall (assessment rating) follows. This sample assessment is on a fictitious local area network that is approved to process SECRET information. A small number of users work in the same environment, yet do not hold a SECRET clearance.

This sample assessment coding scheme is based on the previous page. Keep in mind the following:

Blue	=	Low risk
Green	=	Acceptable risk
Yellow	=	Moderate to high risk
Red	=	High risk

Assessment Coding Scheme	**System Administrator's Manual**
Red	Contains essential guidance to establish, maintain, and operate a secure System or network environment.
Blue	Describes security functions, advisories, warnings, and features.
Blue	Guides log-on activities, authorizing sessions, exchanging information via approved means, and the like.

It appears that Blue outweighs Red; however, the evaluator should have selected Red for the overall rating for this assessment area.

Justification: The system is processing TOP SECRET. All users are not cleared; therefore, they do not have a need-to-know either. The System Administrators must know how to set up, maintain and operate a secure system, given that assurances must be in place that would ensure that users who do not hold a TOP SECRET clearance are not able to gain access.

APPENDIX B: RISK ASSESSMENT CHECKLISTS

RISK ASSESSMENT

These checklists contain the individual risk assessment parameters to be completed as required for your risk assessment type (Survey, Basic, Intermediate, or Full). These checklists include all risk assessment metrics, and based on your risk assessment type, a "Not Applicable" response (or simply leaving the column blank) is appropriate. For each site, network, or system assessed, they capture information from documentation reviews, on-site interviews and observations, and associated analyses. In any case, Designated Approving Authorities (DAAs) are authorized to decide which approach is acceptable within their respective commands.

(Editor's Note: Because the fleet is unique, the fleet should be advised that all Assessment Areas may not apply. Where this is noted as the case, the removal of those Assessment Areas is acceptable. Recommend that they consult their DAA in advance.

1.0 Administrative Assessment Area

Description. [Administration] The procedures, practices, and operating instructions essential to manage and control the system or network mission operations. Also includes procedures for managing consumables such as magnetic tapes, printer paper, and operational supplies. Guidance can be found in DoD 5200.28-STD, Trusted Computer System Evaluation Criteria, and in OPNAVINST 5239.1A, Automated Data Processing Program Handbook. Although outdated, some guidance can be found in the OPNAVINST 5239.1, Automated Data Processing Program Instruction. Additional guidance can be found in the OPNAVINST 5239.xx (Draft) Automated Information Systems Guidelines, various FIPS, and NIST Standards.

Example Security Policy Synopsis . [Documentation Policy]. A cohesive system or network documentation suite shall be prepared, published, and entered into formal configuration management channels. This suite includes the following:

- The manuals identified in this assessment area fall under the DoD umbrella. In some cases, the same information found in a System Administrators Manual can be found in a Standard Operating Procedure or End User's guide, as long as the necessary guidance is documented somewhere. If necessary, the individual performing this assessment can cross out what does not apply and enter in place what would apply.

- User Documentation: System Administrator's Manual, End User's Manual, Standard Operating Procedures, Trusted Facility Manual.

- System Documentation: Configuration Management Plan

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
System Administrator's Manual	B G Y R	
• Contains essential guidance to establish, maintain, and operate a secure system or network environment.	B G Y R	
• Describes security functions, advisories, warnings, and features.	B G Y R	
• Guides log-on activities, authorizing sessions, exchanging information via approved means, and the like.	B G Y R	
• Tailors its language and content appropriately for System Administrators.	B G Y R	
• Avoids *detailed* technical language except where essential to explain cautions and precautions about the provided security functions, features, and measures and their use.	B G Y R	
• Entered into formal configuration management and its distribution *mandatorily* made to each system or network Trusted Official responsible for information resources.	B G Y R	
• Describes how the system administrator is able to modify message headers.	B G Y R	
• Guides administrator on how to assign a subject privilege that would allow him/her to reassign down to group user.	B G Y R	
(System Administrator's Manual) Assessment Area Rating		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
End User's Manual	B G Y R	
• Contains adequate guidance for establishing, maintaining, and operating a secure workplace environment for system or network supported tasks.	B G Y R	
• Describes security functions, advisories, warnings, and features.	B G Y R	
• Guides user on log-on activities, conducting sessions, exchanging information via approved means, and the like.	B G Y R	
• Tailors guidance for the several End User groups (e.g., Budgeting, Accounting).	B G Y R	
• Avoids technical *details* except where essential to explain cautions and precautions about the provided security functions, features, and measures and their use.	B G Y R	
• Entered into formal configuration management and its distribution *mandatorily* made to each Network End User (e.g., Functional User, Functional User Group member).	B G Y R	
(End User's Manual) Assessment Area Rating		
Trusted Facility Manua l		

• Contains precautions about privileges and functions to be controlled when running a secure facility. • Provides procedures for examining and maintaining audit trails. • Provides procedures for the System Operator and System Administrator. This shall include those security privileges that they have authority to modify.	B G Y R B G Y R B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
(Trusted Facility Manual) Assessment Area Rating		
Standard Operating Procedures • Documents security procedures developed or tailored for a system or network. • Provides instructions for generating, storing, controlling, and destroying sensitive output products and residual by-products. • Addresses, for example, safeguarding system or network hardware and software, procedures for reporting potential security problems or discovered flaws, suggested security improvements, instructions about protecting *Privacy Act* information, and so on.	B G Y R B G Y R B G Y R B G Y R	
(Standard Operating Procedures) Assessment Area Rating		
Operational Consumables • Procedures address how to acquire, account for, and stock adequate supplies of: - Diskettes [disks] - Tapes - Printer paper - Other essential supplies_____	B G Y R B G Y R B G Y R B G Y R B G Y R B G Y R	
(Operational Consumables) Assessment Area Rating		

OVERALL ASSESSMENT (ADMINISTRATIVE) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
System Administrator's Manual		
End User's Manual		
Trusted Facility Manual		
Standard Operating Procedures		
Operational Consumables		

2. Communications Assessment Area

Description. [Communications] The transcontinental and similar circuits used by this site, command, facility, and/or directorate, in support of mission objectives. Also includes the wide area and/or local area network plant and equipment. Guidance can be found in DoD 5200.28-STD, Trusted Computer System Evaluation Criteria.

Example Security Policy Synopsis [Communications Security (COMSEC)]. COMSEC guards against disclosing sensitive or classified information flowing on communications circuits by protecting them with cryptographic or other approved techniques. COMSEC rules given in National Security Decision Directive 145, (S) *National Policy on Telecommunications and Automated Information Systems Security* (U), shall be addressed for applicability during Risk Assessment activities. At a minimum, network communications circuits shall be given sufficient Transmission Security protection to counter unauthorized tampering or other penetration attempts.

Network Security extends system-enforced safeguard protection features to networks and their components. Through special techniques (services), it establishes controls (mechanisms) for performing identification and authentication, implements access controls over interfaced systems and users, and audits user activity conducted through network-provided services. NCSC-TG-500, Trusted Network Interpretation, applies. Various FIPS PUBS are also available that relate to networks such as FIPS PUB 107, 146-1, and 179.

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Circuit Identifiers	B G Y R	
• Trunking assignment(s) identified with regard to major supported capabilities, and connectivity to routers or other essential communications assets.	B G Y R	
• Communications circuit identifiers posted with each circuit to expedite restoration and trouble-shooting efforts.	B G Y R	
• Connectivity topology known, published, and made readily available for technical control activities.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
(Circuit Identifiers) Assessment Area Rating		
Local Area Network and/or Wide Area Networks	B G Y R	
• Computer port(s) use identified (e.g., router assignments, storage resources).	B G Y R	
• *Foreign Domain* network(s) and their associated computer port(s) identified thus explicitly distinguishing between *internal domain* and *foreign domain* assets.	B G Y R	
• CISCO™ Routers/any other Router Configurations have been reviewed for known vulnerabilities.	B G Y R	
• Packets are filtered to prevent flooding or traffic flow problems on the network.	B G Y R	
• Routers are configured to filter incoming packets based on network address so that only packets from authorized trusted sites are allowed to enter the network.	B G Y R	
• Modem pools are set up and monitored.	B G Y R	
• Servers with back-door entries into the Internet or other foreign networks are audited.	B G Y R	
• Designated officials are assigned with alternates for bringing routers back on line after a fault.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Procedures are in place for altering users to intrusions and/or manipulation of network assets. • Encryption is used between the sending node/process and receiving node/process to ensure traffic flow confidentiality service. • Bridges and routers are used in network configuration to restrict certain addresses from subnets.	B G Y R B G Y R B G Y R	
(Local Area Network and/or Wide Area Networks) Assessment Area Rating		
Physical Protection and Operational Continuity • Communications "closets" secured to restrict access to authorized persons only. • Tamper-resistant seals defend against surreptitious tampering.	B G Y R B G Y R B G Y R	
(Physical Protection and Operational Continuity) Assessment Area Rating		
-- r e s e r v e d --		

OVERALL ASSESSMENT (COMMUNICATIONS) AREA		
Assessed Areas	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Circuit Identifiers		
Local Area Networks and/or Wide Area Networks		
Physical Protection and Operational Continuity		

3. Emanations Assessment Area

Description. [Emanations] The unintended intelligence bearing or interfering signals emitted from properly functioning system or network computers, peripherals, signal lines, communications circuits, and other equipment.		
Example Security Policy Synopsis . [Emanations Security (EMSEC)]. EMSEC, also known as TEMPEST, prevents exploiting intercepted electromagnetic energy radiated from equipment that processes sensitive or classified information. EMSEC guidance shall be used to guide equipment placement and installation practices to minimize signal interference from [or to] other equipment or system components. This applies regardless of whether processing classified or unclassified. Guidance can be found in OPNAVINST C5510.93E.		
Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Installation Practices	B G Y R	
• Cable routing and placement minimize signal interference hazards.	B G Y R	
• Rack or equipment bays placement minimizes signal interference hazards.	B G Y R	
• Single station ground practices minimize "ground loop" signal coupling and associated safety hazards.	B G Y R	
• Safety regulations followed (e.g., high-voltage warning signs). Overall Rating for (Installation Practices) Assessment Area .	B G Y R	
(Installation Practices) Assessment Area Rating		
TEMPEST (classified systems only)	B G Y R	
• If appropriate, TEMPEST Vulnerability Assessment Request has been submitted.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Red/Black criteria have been met for non-TEMPEST approved systems. • Protective Distribution Systems are in place for those systems processing with signal lines running through uncleared spaces. • If appropriate, TEMPEST Vulnerability Request submitted to appropriate authority.	B G Y R B G Y R B G Y R	
(TEMPEST) Assessment Area Rating		
-- r e s e r v e d --		

OVERALL ASSESSMENT (EMANATION) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Installation Practices		
TEMPEST		

4. Information Assessment Area

Description. [Information] The data whether "raw" or "processed" used in support of the mission statement objectives. Guidance can be found in OPNAVINST 5510.1H, Information and Personnel Security Regulations; and various FIPS and NIST Standards.

Example Security Policy Synopsis . Information Security guards against actual or potential information loss through a combination of administrative policies and procedures, which alert people to a product's sensitivity or handling restrictions. It also establishes the need to account for, store, and destroy such information as prescribed by basic information security regulations.

* Side Note for Fleet. The term Security Officials is synonymous with Security Staff. Information Storage, Handling, and Destruction are incorporated in User's Manuals.

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Responsible Security Official(s)	B G Y R	
• Responsible security official(s) designated, in writing, for	B G Y R	
- Information and resources	B G Y R	
- User workplace information and resources.	B G Y R	
(Responsible Security Officer) Assessment Area Rating		
Information Sensitivity	B G Y R	
• Processed information explicitly identified for protection as:	B G Y R	
- Privacy Act information or resources (e.g., personal, personnel)	B G Y R	
- For Official Use Only information or resources (e.g., financial)	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
- Information or resources needed to accomplish activity mission and business process responsibilities	B G Y R	
- Publicly held or available information or resources.	B G Y R	
(Information Sensitivity) Assessment Area Rating		
Information Access Controls	B G Y R	
• Information access controls are based on security policy rules for the following:	B G Y R	
- Access requires official duty task assignment(s)	B G Y R	
- Accountability for control traceable to a single individual	B G Y R	
- Explicit privilege mandatorily granted; no default access.	B G Y R	
• System terminals display a "system prompt" before the user has signed onto the system.	B G Y R	
• System terminals display a "log on prompt" before the user has signed onto the system.	B G Y R	
• Procedures are in place to ensure that upon completion of subject task the group user is disabled.	B G Y R	
(Information Access Controls) Assessment Area Rating		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Information Storage, Handling, and Destruction • Information storage, handling, and destruction procedure documentation addresses: - Guidance tailored for system or network in System Administrator's Manual - Guidance tailored for system or network in End User's Manual - Guidance otherwise in site instruction. • System backups are performed regularly. • Backup media are stored off site along with copy of contingency plan (e.g., off-site - is defined as any building other than where the equipment is located).	B G Y R B G Y R B G Y R B G Y R B G Y R B G Y R B G Y R	
(Information Storage, Handling, and Destruction) Assessment Area Rating		
-- r e s e r v e d --		

OVERALL ASSESSMENT (INFORMATION) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Area**
Responsibility Security Official(s)		
Information Sensitivity		
Information Access Controls		
Information Storage, Handling, and Destruction		

5. Logistics Assessment Area

Description. The documentation, plans, procedures, and other material needed to install, initialize, and operate system or network components. Also includes Central Design Activity and Software Support Activity capabilities essential to provide adequate life-cycle support.		
Example Security Policy Synopsis . [Assurance Element Policy]. Assurances that System or network's security protection measures have been faithfully implemented shall be sufficient to convincingly sustain informed decisions leading to operational fielding via the certification and accreditation processes. • Assurances - Developmental Assurances - Operational Assurances • Risk Assessment • Contingency Planning.		
Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Developmental Assurances	B G Y R	
• Formal reviews conducted and actions documented.	B G Y R	
• Appropriate functional testing done, results documented, and corrections taken based on:	B G Y R	
- Unit tests	B G Y R	
- Functionality tests	B G Y R	
- System tests.	B G Y R	
• Appropriate security testing done, results documented, and corrections taken for:	B G Y R	
- Identification and Authentication features	B G Y R	
- Discretionary Access Control features	B G Y R	
- Security Audit Trail features	B G Y R	
- Object Reuse Features	B G Y R	
- Control "scripts" and/or "shells" features (verified and approved).	B G Y R	
(Developmental Assurance) Assessment Area Report		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Operational Assurances	B G Y R	
• Formal configuration management procedures ensure authorized configuration(s) remain unconditionally stable.	B G Y R	
• Diagnostics provide periodic confidence checks.	B G Y R	
• Text fixtures removed prior to releasing master load media to field sites.	B G Y R	
• Appropriate security "confidence" check-out tests conducted to ensure installation completed properly.	B G Y R	
• Problem reports analyzed, corrective actions taken, and certification posture reviewed for potential impact.	B G Y R	
(Developmental Assurance) Assessment Area Report		
Life-Cycle Assurances	B G Y R	
• Software Support Activity identified and serving in an approved role.	B G Y R	
• Contingency planning:	B G Y R	
- Appropriately documented - Practiced at scheduled intervals - Lessons learned incorporated.	B G Y R B G Y R B G Y R	
(Life Cycle Assurance) Assessment Area Report		
Viruses	B G Y R	
• Incident Reporting Procedures in place (applies to viruses and intruders)	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Virus scanning software installed on systems to ensure malicious code is not introduced into systems (e.g., trojan horse). • Files are automatically scanned before attached to e-mail messages.	B G Y R B G Y R	
(Viruses) Assessment Area Report		
Accreditation • Plan published and approved; plan execution underway [or completed]. • Accreditation Support Package underway [or completed and approved]. • Formal signature(s) obtained on Accreditation Support Package.	B G Y R B G Y R B G Y R B G Y R	
(Accreditation) Assessment Area Report		
-- r e s e r v e d --	B G Y R	

OVERALL ASSESSMENT (LOGISTIC) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Developmental Assurances		
Operational Assurances		
Life-Cycle Assurances		
Viruses		
Accreditation		

6. Network Assessment Area

Description. The hardware, software, communications circuits, operational practices, and other components that collectively constitute network mission support capabilities.

Example Security Policy Synopsis .

- [Network Security (NETSEC)]. NETSEC extends system-enforced safeguard protection features to networks and their components. Through special techniques [services], it establishes controls [mechanisms] for performing identification and authentication, implements access controls over interfaced systems and users, and audits user activity conducted through network-provided services. Techniques for Network security functions shall be detailed in the *Network Security Policy*.
- [Operations Security (OPSEC)]. OPSEC denies sensitive information to hostile agents by identifying, controlling, and protecting indicators associated with planning and conducting departmental sensitive activities. Guidance provided in NIST Pub #500-171, *Computer User's Guide to the Protection of Information Resources*, applies to Network.

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Connectivity Services	B G Y R	
• Network Connectivity Services documentation explicitly identifies physical pathway(s) through network topology.	B G Y R	
• Network Connectivity Services guard against requests that would result in illogical pathway(s) through network topology.	B G Y R	
• Network Connectivity Services explicitly identify and control privileged pathway(s) through network topology, if any.	B G Y R	
(Connectivity Services) Assessment Area Report		
Transport Services	B G Y R	
• System or network Transport Services integrity features protect against "tampering" or other unauthorized data modification attacks.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• System or network Transport Services confidentiality features safeguard data exchanges against unauthorized disclosure attacks.	B G Y R	
• System or network Transport Services integrity features ensure:	B G Y R	
- End-to-end exchange delivery occurs	B G Y R	
- Appropriate error notification occurs.	B G Y R	
• Is message integrity confirmed at recipient system. (Is the message sent what was received at the far end?)	B G Y R	
(Transport Services) Assessment Area Report		
Name Server Services	B G Y R	
• Network Name Server features associate "named users" with protected Network resources to their individual:	B G Y R	
- *Community-of-interest* assignment(s)	B G Y R	
- Granted privilege set(s)	B G Y R	
- Authorized connectivity assignment(s)	B G Y R	
- Access mode(s).	B G Y R	
(Name Server Services) Assessment Area Report		
Internet Server Services	B G Y R	
• Network Internet Server features:	B G Y R	
- Restrict "in-coming" and "outgoing" exchanges consistent with authorized *community-of-interest* privilege assignment(s) associated with an exchange.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
- Defend against *foreign domain* to *foreign domain* exchanges via *corporate* trunks.	B G Y R	
(Internet Server Services) Assessment Area Report		
Terminal Server Services	B G Y R	
• Network Terminal Server services safeguard against password interception attacks via authentication mechanism(s) "stronger than" static password techniques for:	B G Y R	
- Local call privileges	B G Y R	
- Data exchanges using *corporate* trunking.	B G Y R	
(Terminal Server Services) Assessment Area Report		
Network Registration Services	B G Y R	
• Network Registration features allow designated Network Trusted Officials (e.g., *Administrator*) to register candidate users and to explicitly establish their:	B G Y R	
- *Community-of-interest* assignment(s)	B G Y R	
- Granted privilege set(s)	B G Y R	
- Permitted access mode(s).	B G Y R	
(Network Registration Services) Assessment Area Report		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Network Identification and Authentication Services	B G Y R	
• Network identification and authentication features provide "notarized" identification and authentication services to requesting information systems (e.g., honor requests to verify a user's claimed identity).	B G Y R	
• The system/component supports enhanced identification and authentication with dialups and/or network access.	B G Y R	
• The system/component supports dialups and/or network access.	B G Y R	
(Network Identification and Authentication) Assessment Area Report		
Network Access Control Services	B G Y R	
• Network Access Control features adjudicate, via computer-enforced safeguard techniques, requested access to protected network resources by:	B G Y R	
· Community-of-interest assignment(s).	B G Y R	
· Granted privilege set(s).	B G Y R	
· Permitted access mode(s).	B G Y R	
(Network Access Control Services) Assessment Area Report		
Network Auditing Services	B G Y R	
· Network Auditing features record [permit recording] security related events, such as:	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
- Acts by Trusted Officials (e.g., grant privileges, assign community-of-interest)	B G Y R	
- Access attempts, successful or not, upon protected network resources (e.g., log-on failures, successfully forward data to designated business center server(s))	B G Y R	
- Unauthorized access attempts (e.g., ungranted privilege(s))	B G Y R	
- Unauthorized access mode attempts (e.g., write to a read-only resource, execute an application not permitted by community-of-interest rules)	B G Y R	
- Breached computational resource thresholds.	B G Y R	
(Network Auditing Services) Assessment Area Report		
Network Monitoring Services	B G Y R	
• Network monitoring features forward abnormal "indicators" to the network Monitoring Center for review and disposition:	B G Y R	
- "Failed" log-in attempts	B G Y R	
- Unauthorized access attempts (e.g., ungranted privilege(s))	B G Y R	
- Computational resource threshold(s) reached	B G Y R	
- Actual or suspected (malicious or not) penetration attempts.	B G Y R	
(Network Monitoring Services) Assessment Area Report		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Network Operations Security Services • Network Operations Security procedures appropriately defend against revealing: - Sensitive or privileged operational plans, capabilities, or limitations.	B G Y R B G Y R B G Y R	
(Network Operations Security Services) Assessment Area Report	B G Y R	
-- r e s e r v e d --	B G Y R	

OVERALL ASSESSMENT (NETWORK) AREA		
Assessed Areas	**Overall Color Code Rating**	**List Critical Vulnerability for Each Area**
Connectivity Services		
Transport Services		
Name Server Services		
Internet Server Services		
Terminal Server Services		
Network Registration Services		
Network Identification and Authentication Services		

Assessed Areas	Overall Color Code Rating	List Critical Vulnerability for Each Area
Network Access Control Services		
Network Auditing Services		
Network Monitoring Services		
Network Operations Security Services		

7. Personnel Assessment Area

Description. The people who operate, maintain, manage, or use system or network in its mission supporting role.		
Example Security Policy Synopsis . [Personnel Security (PERSEC)]. PERSEC ensures people who require access to sensitive information have been properly and formally authorized for that access. The policies contained in *(sample)* Instruction 731-1, Personnel Security/Suitability Policy and Technical Guidance, apply to the *(sample) corporate* information resources and capabilities. All system or network users, whether functional *community-of-interest* members or interfaced computer systems, SHALL have appropriate authorization(s) e.g., official duty task assignment(s) verified before being permitted to access its information or invoke its capabilities.		
Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Functional Users	B G Y R	
• PERSEC verifications ensure that functional users are bona fide employees or sponsored for essential tasks.	B G Y R	
• PERSEC verifications ensure official duty task assignment(s) require system or network access.	B G Y R	
• PERSEC training conducted on security responsibilities and obligations.	B G Y R	
(Functional Users) Assessment Area Report		
Functional User Group Members	B G Y R	
• PERSEC verifications ensure candidate functional user group members are bona fide employees or sponsored for essential tasks.	B G Y R	
• PERSEC verifications ensure official duty task assignment(s) require system or network access.	B G Y R	
• PERSEC training conducted on security responsibilities and obligations.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
(Functional User Group Members) Assessment Area Report		
Trusted Officials	B G Y R	
• PERSEC verifications ensure candidate Trusted Officials (e.g., System Operator, Terminal Area Security Officer) are bona fide employees only.	B G Y R	
• PERSEC verifications ensure official duty task assignment(s) **require** Trusted Official access and associated privileges.	B G Y R	
• PERSEC training conducted on Trusted Official responsibilities and obligations.	B G Y R	
(Trusted Officials) Assessment Area Report		
-- r e s e r v e d --	B G Y R	

OVERALL ASSESSMENT (PERSONNEL) AREA

Assessed Areas	Overall Color Code Rating	List Critical Vulnerability for Each Assessed Area
Functional Users		Remarks
Functional User Group Members		
Trusted Officials		

8. Physical Assessment Area

Description. The rooms, buildings, and structures housing system or network equipment. Also includes sustaining environmental systems such as power, light, air handling, and protected storage (e.g., appropriate countermeasures against theft, abuse, and inadvertent damage).		
Example Security Policy Synopsis . [Physical Security (PHYSEC)]. PHYSEC wards off intrusions into sensitive work areas and guards against resource theft, destruction, or tampering by establishing physical control zones that require formally granted permission to enter and gain unescorted access. The provisions in FIPS Pub #31, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, apply to system or network.		
Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Facility	B G Y R	
• Appropriately designated as *Restricted Area* or *Controlled Access Area*.	B G Y R	
• Site selection enhances security and promotes operational mission utility.	B G Y R	
• Responsible security official(s) designated, in writing.	B G Y R	
• Access roster and appropriate badging system in place.	B G Y R	
• Housekeeping fosters security and safety.	B G Y R	
(Facility) Assessment Area Report		
Operations Area	B G Y R	
• Appropriately designated as *Restricted Area* or *Controlled Access Area*.	B G Y R	
• Site selection enhances security and promotes operational mission utility.	B G Y R	
• Responsible security official(s) designated, in writing.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Access roster and appropriate badging system in place. • Housekeeping fosters security and safety.	B G Y R B G Y R	
(Operations) Assessment Area Report		
Communications Closet • Appropriately designated as *Restricted Area* or *Controlled Access Area*. • Site selection enhances security and promotes operational mission utility. • Responsible security official(s) designated, in writing. • Access roster and appropriate badging system in place. • Housekeeping fosters security and safety.	B G Y R B G Y R B G Y R B G Y R B G Y R B G Y R	
(Communications Closet) Assessment Area Report		
Functional User Workplace • When applicable, appropriately designated as *Restricted Area* or *Controlled Access Area*. • Site selection enhances security and promotes operational mission utility. • Responsible security official(s) designated, in writing. • Access roster and appropriate badging system in place. • Housekeeping fosters security and safety.	B G Y R B G Y R B G Y R B G Y R B G Y R B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
(Functional User Workplace) Assessment Area Report		
-- r e s e r v e d --		

OVERALL ASSESSMENT (PHYSICAL) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Facility		
Operations Area		
Communications Closet		
Functional User Workplace		

9. Software Assessment Area

Description. The operating systems, application programs, and key utility programs needed for the system or network to perform its mission functions.
Example Security Policy Synopsis . [System-Enforced Safeguard Element Policy]. FIPS Pub # 73, *Guidelines for Security of Computer Applications*, and *(sample)* Circular #10, *Automated Information Systems Security Program*, describe the safeguard features and functionality essential to protect sensitive information handled by a computer system. For system or network, these rules apply. • Registration Rule. No access unless registered on the system by cognizant Trusted Officials (e.g., System Administrator). • Identification and Authentication Rule. No access unless identified and authenticated. • Discretionary Access Control Rule. Granted explicit privileges to do so by Trusted Officials (e.g., System Administrator) -- *exception e-mail.* • Security Audit Trail Rule. Act or attempted act recorded *[recordable]* in the Security Audit Trail.

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Registration Rule	B G Y R	
• No default "users" exist (e.g., guest, anonymous).	B G Y R	
• Official duty mission task assignment(s) required and verified.	B G Y R	
• Explicit registration required for:	B G Y R	
- People (including Trusted Officials)	B G Y R	
- Protected resources (e.g., financial data)	B G Y R	
- Privileged programs (e.g., exchange data file)	B G Y R	
- Controlled capabilities (e.g., access archive library)	B G Y R	
- Electronic entities (e.g., interfaced systems, communications ports).	B G Y R	
• Passwords are issued in a secure manner to preclude disclosure.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
(Registration Rule) Assessment Area Report		
Identification and Authentication Rule	B G Y R	
• Passwords checked for triviality against "strong" criteria.	B G Y R	
• Installation and vendor "standard" passwords removed.	B G Y R	
• Group passwords limited to essential mission functions.	B G Y R	
• Registration passwords set to "expired."	B G Y R	
• Appropriate password aging rules established and followed.	B G Y R	
• *Navy approved Warning Banner...* displayed prior to completing log-on.	B G Y R	
• Dialups/remote access is supported with enhanced identification and authentication.	B G Y R	
• System administrators are able to assign ownership and execute privileges to a subject, yet disallow others access to that group's objects.	B G Y R	
• Users who are not assigned ownership and execute privileges to objects can still gain access to the object.	B G Y R	
• Is access to an object restricted to the owner by default?	B G Y R	
• The system disables the terminal upon entering set amounts of invalid user IDs (e.g., four or five failed attempts).	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Password files are encrypted such that not even the system administrator or root administrator can read them in the clear.	B G Y R	
• All application passwords are protected (with unique passwords, indifferent from those used during initial system log-on.)	B G Y R	
• System terminals display a "system prompt" before the user has signed onto the system.	B G Y R	
• System terminals display a "log-on prompt" before the user has signed onto the system.	B G Y R	
• Assessment Metric(s) (Potential Vulnerabilities).		
• Procedures are in place to ensure that upon completion of subject task, the group user is disabled.	B G Y R	
• Terminal disabled upon entering (x) set amounts of invalid user IDs (e.g., four or five failed attempts).	B G Y R	
• Password files are encrypted such that not even the system administrator or root administrator can read them in the clear.	B G Y R	
(Identification and Authentication Rule) Assessment Area Report		
Discretionary Access Control Rule	B G Y R	
• Access mode privileges enforced (e.g., read, write, execute, and search).	B G Y R	
• No "default" access permitted.	B G Y R	
• Communications ports protected by appropriate privilege.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Dial-in ports have additional privilege required to access.	B G Y R	
• Data owners provide "internal" warning banners within data stream (e.g., Privacy Act).	B G Y R	
• System administrators are able to assign ownership and execute privileges to a subject, yet disallow others access to that group's objects.	B G Y R	
• Users who are not assigned ownership and execute privileges to objects can still gain access to the object.	B G Y R	
• Is access to an object restricted to the owner by default?	B G Y R	
• The system disables the terminal upon entering set amounts of invalid user (IDs (e.g.. four or five failed attempts).	B G Y R	
• Password files are encrypted such that not even the system administrator or root administrator can read them in the clear.	B G Y R	
• All application passwords are protected (with unique passwords, indifferent from those used during initial system log-on.	B G Y R	
(Discretionary Access Control Rule) Assessment Area Report		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Security Audit Trail Rule	B G Y R	
• The system administrator log-on and log-off activities recorded in audit trail.	B G Y R	
• As applicable (output has classification labels).	B G Y R	
• Session parameters recorded [recordable] (e.g., log-in ID, date, time, and terminal).	B G Y R	
• File(s) and access mode(s) recorded [recordable].	B G Y R	
• Capabilities invoked recorded [recordable] (e.g., modify, delete, or execute).	B G Y R	
• Unauthorized access attempts recorded [recordable].	B G Y R	
• Administrative and security relevant actions taken by Trusted Officials recorded.	B G Y R	
• System-enforced features "clear" storage areas being "recycled" by the system.	B G Y R	
-- r e s e r v e d --		
Overall Rating for (Discretionary Access Control Rule) Assessment Area		

OVERALL ASSESSMENT (SOFTWARE) AREA		
Assessed Areas	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Registration Rule		
Identification and Authentication Rule		
Discretionary Access Control Rule		
Security Audit Trail Rule		

10. UNIX Security Assessment Area

Description. The software, configuration files, operating parameters, and services associated with computers using the UNIX operating system to provide network services.		
Example Security Policy Synopsis . [UNIX Network Security.] UNIX Network Security provides a secure network operating environment where systems using the UNIX operating system provide network transport, name service, auditing, and firewall features. UNIX networking nodes must be established and configured in such a manner that not only are intrusions, theft, sabotage, and spoofing kept to a minimum, but also a means is employed to discover unauthorized intrusions and allow recreation of events leading up to that intrusion.		
Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Securing UNIX Systems (some preventive measures)	B G Y R	
• Passwords are placed on root accounts.	B G Y R	
• The /etc/hosts.equiv file is removed or configured to trust specific host.	B G Y R	
• The tftp, rsh, rexec, rusers in /etc/inetd.conf commands are disabled.	B G Y R	
• The shells of unused accounts in /etc/passwd are replaced with /bin/false.	B G Y R	
• The /etc/exports file is removed or configured to export to specific host.	B G Y R	
• Supplemental system security patches are installed (if applicable).	B G Y R	
• Ensure that the following is performed (AFTER EVERY REBOOT): "chmod 644 /etc/utmp and /etc/motd."	B G Y R	
• The chmod 666 should be "chmod 644 /etc/motd" in /etc/rc.local.	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• Create /etc/ftpusers file to contain (root nobody daemon sys binuucp news ingres audit sync sysdiag sundiag).	B G Y R	
• The command "secure" is removed from /etc/ttytab (maybe not console).		
• Ensure the DoD log-in banner is installed in the (/etc/motd).	B G Y R	
• The following groups are assigned (/etc/netgroup and /var/yp/etc/netgroup).	B G Y R	
• The following user accounts are removed from the password file (news ingres sysdig sundiag).	B G Y R	
• Screenblank is added to /etc/rc.local.	B G Y R	
• Sendmail lines are moved to end of /etc/rc.local and add appropriate options.	B G Y R	
• Domain print has been removed from /etc/sendmail.cf.	B G Y R	
• Network Information System (NIS)	B G Y R	
- Ensure that /var/yp/etc have been created	B G Y R	
- Copy appropriate /etc files into var/yp/etc (passwd, osts, ethers, group, networks, protocols, services, bootparams)	B G Y R	
- Ensure that (+::0:::) is removed from /var/yp/etc/group and /var/yp/etc/passwd file)	B G Y R	
- Ensure the following is modified: (/var/yp/Makefile DIR variable to DIR=/var/yp/etc	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
- Ensure /var/yp/Makefile B= variable to B+-b	B G Y R	
- UNIX file protection mechanisms active	B G Y R	
- Identify SUI and SGI files on the system	B G Y R	
- These files allow an unprivileged user to accomplish tasks that require privileges		
- Users can change the ownership of an SUI or SGI file and "give away" these files to root	B G Y R	
- Current directory is not included in the search path for root and writable by others	B G Y R	
- Root's startup files are only writable by root	B G Y R	
- Only legitimate files are world-writable.	B G Y R	
• Only authorized device files are on the system.	B G Y R	
• Filesystem is only mounted with the suid option if there is a legitimate business need.	B G Y R	
• Filesystem is exported with read-only whenever possible.	B G Y R	
• Shell resets the IFS variable when the shell is invoked.	B G Y R	
• Other generic UNIX Systems.	B G Y R	
• COPS, SPI, and Tripwire are run periodically.	B G Y R	
(Securing <u>SUN</u> Systems (some preventive measures)) Assessment Area Rating		

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
Auditing **(UNIX environment)**	B G Y R	
• The audit trail is capable of tracking the following events: - Use of I&A mechanisms, i.e., logon - Introduction of objects into a user's address space (file open, file creation, program execution, and file rename) - Deletion of objects from a user's address space (file close, completion of program execution, and field deletion) - All security relevant events (use of privileges, changes to DAC parameters) - Producing printed output.	B G Y R	
• All auditable events should record the following information: - Date and time of the event - Unique identifier of the user's program generating the event was operating - Type of event - Success or failure of the event - Origin of the request, (e.g., terminal identifier for I&A events) - Name of the object that was introduced into or deleted from the user's address space - Description of modifications that the system administrator makes to a security database.	B G Y R	
• Syslog is activated for auditing, and the disk/hard copy logs are reviewed on a regular basis by system management for violations/anomalies.	B G Y R	
• Accounting program is turned on to log the use of "UNIX commands."	B G Y R	

Assessment Metric(s) (Potential Vulnerabilities)	Assessment	Countermeasure Required and/or Remarks
• All patches/fixes have been installed to correct previously reported security vulnerabilities.	B G Y R	
(Auditing) Assessment Area Report		
Firewalls	B G Y R	
• Firewalls have been installed on the network to stop or reduce malicious damage and intrusion.	B G Y R	
• Bridges and routers are used in the network configuration as packet filters to restrict certain network traffic from passing beyond certain domains or subnetworks.	B G Y R	
• Application Gateways/bastion hosts with proxies are used in the network configuration to serve as chokepoints through which network traffic must traverse for identification, authentication of users, and audit logging.	B G Y R	
(Firewalls) Assessment Area Report		
-- r e s e r v e d --	B G Y R	

OVERALL ASSESSMENT (UNIX SECURITY) AREA		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability for Each Assessed Area**
Securing UNIX Systems		
Auditing		
Firewalls		

OVERALL SUMMARY OF ASSESSED AREAS		
Assessed Area	**Overall Color Code Rating**	**List Critical Vulnerability For Each Assessed Area**
Administrative Area		
Communications Area		
Emanations Area		
Information Area		
Logistics Area		
Network Area		
Personnel Area		
Physical Area		
Software Area		
UNIX Security Area		