# Chapter 6

# Configuration Management for Classified Equipment

## Introduction

The complexity of a configuration management (CM) program depends, as does many other issues, on what is defined as an automated information system (AIS). An AIS is not, strictly speaking, a single computer system. An AIS is an assembly of computer hardware, firmware and software that is configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information. The AIS, therefore, can consists of many components which work together to form a single function. This single function theory forms the basis for the configuration management controls that have evolved in various organizations.

## Scope

This chapter evaluates configuration management requirements and associated life-cycle management needs, plus techniques employed by various organizations to control equipment used for classified data processing. Configuration management requirements are imposed on networked and stand-alone, sometimes TEMPEST-approved, automated information systems (AISs). The study will focus on primarily personal computers and computer workstations usually intended for a classified processing environment. Organizational comparisons are included in Appendix A.

***INTRODUCTION***

***An AIS is not, strictly speaking, a single computer system.***

***An AIS is an assembly of hardware, firmware and software that is configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information.***

***An AIS consists of many components which work together to form a single function.***

***This single function theory forms the basis for the configuration management controls.***

## Introduction to Configuration Management

Configuration management consists of identifying, controlling, accounting for, and auditing all changes made to a particular system or equipment during its life cycle. In particular, as related to equipment used to process classified information, equipment can be identified in categories of COMSEC, TEMPEST, or as a Trusted Computer Base (TCB).

***CM DEFINITION***

***Configuration management consists of identifying, controlling, accounting for, and auditing all changes made to system during its life cycle.***

***Equipment used to process classified information can be identified in categories of COMSEC, TEMPEST, or as a Trusted Computer Base (TCB).***

The Trusted Computer System Evaluation Criteria (TCSEC) requires all changes to the TCB for classes B2 through A1 be controlled by configuration management. Although the "rainbow series" documentation mostly relates to software controls for trusted computers, configuration management is not limited to only this function.  The TCSEC gives the following as the Assurance Control Objective:

> "Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy.  Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life cycle."

## What Does Configuration Management Mean?

Configuration management can be thought of as a quality-assurance (QA) discipline which incorporates aspects involving both identification and authentication of objects within a system.  It controls changes to system software, firmware, hardware, and documentation throughout the life of the AIS.  This includes the design, development, testing, distribution, and operation of modifications and enhancements to the existing system.  More specifically, configuration management applies direction to: 1) identify and document the functional and physical characteristics of each configuration item for a product; 2) manage all changes to these characteristics; and 3) record and report the status of change processing and implementation.  In other words, configuration management is the means used to protect a system against unauthorized modifications, and ensures that all protection properties of a system work only as intended and are maintained after an authorized modification takes place.

***What Does CM Mean?***

***CM can be thought of as a QA discipline which incorporates both identification and authentication of objects within a system.***

***It controls changes to system software, firmware, hardware, and documentation throughout the life of the AIS.***

***CM TASKS***

***1) Identification:  identify and document the functional and physical characteristics of each configuration item for a product***

***2) Control:  manage all changes to these characteristics***

***3) Status Accounting and Audit:  record and report the status of change processing and implementation.***

Configuration management is really a process of engineering sound and secure operating practices into the AIS.  As such, controls are placed on AISs to insure that every change in hardware, software, firmware, operational procedures, or documentation is verified and approved by the authorized or controlling party for the AIS.  These security controls can be broken down into four separate tasks:  identification, control, status accounting, and auditing.  These tasks are applied through various techniques to ensure correct operation of the system.

## Life-Cycle Management

Life-Cycle Management (LCM) is applied to programs, projects, and activities concerned with the design, development, deployment, and operation computing and telecommunications resources. Formal LCM is a control process applied by DoD directive[1] to expenditures on new information systems, and to expenditures on the modernization of existing systems. Control decisions for all expenditure are based on the total anticipated benefits that will be derived over the life of the new system, or, that will be derived over the life of a modified and improved information system.

LCM is used to control expenditures on new or upgraded systems to ensure that the benefits derived cost effectively satisfy mission needs to the greatest extent possible. For information security, LCM is intended to safeguard information resources using prescribed protective measures and controls to meet the specified security requirements. Information policy and procedures, functional requirements, information flows, information technology, telecommunications, security requirements, and other elements are integrated into the planning and evaluation of each alternative program concept.

***LCM Phases***

***Phase 0: Need Justification Phase***

***Phase 1: Concepts Development Phase***

***Phase 2: Design Phase***

***Phase 3: Development Phase***

***Phase 4: Deployment Phase***

***Phase 5: Operations Phase***

## Technology Life-Cycle

Technology life-cycle (TLC) describes the value gain of a product through the expense of research and development phase, and the financial return during its "vital life". Information technologies have a relatively short lifespan requiring constant re-evaluation an improvement to keep abreast of industry enhancements or threat increases.

Within the commercial world, technology life cycle is concerned with the time and cost of developing the technology, the timeline of recovering cost, and modes of making the technology yield a profit proportionate to the costs and risks involved. In the information security world, particularly in DoD, life-cycle is concerned with continued protection of mission assets through reliability, availability and maintainability, the “RAM” process. Figure 1 depicts the traditional TLC process.

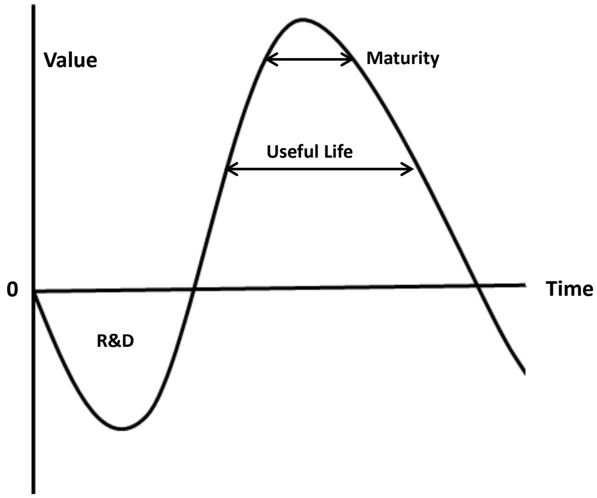

**Figure 1 – Technology Life-Cycle**

## Software Life-Cycle

Unfortunately, software is only as secure as the ability of the developers to make it secure. Historically, applications are developed in a way

[1] ***NUAIBER 7920.1, Life-Cycle Management of Automated Information Systems (AlSs);NUIBER 7740.1, DoD Information Resources Management Program; DoDD 5000.1, Major and Non-Major Defense Programs Acquisitions***

that doesn't always ensure that all vulnerabilities are mitigated prior to its release, particularly in the world of commercial-off-the-shelf (COTS) solutions. For this reason, many applications require continuous improvements (called patch management) to enhance their secure operational characteristics. Additionally, a host of external protection mechanisms have evolved to help further protect these applications from internal and external threats.

***TRACEABILITY***

***Traceability extends from the initial system baseline through the system's entire life cycle.***

***Once something is designated a configuration item early in the system's development, every change must be under CM control.***

**Configuration Item Identification**

The function of configuration item identification is to identify the components of a system for traceability. As such, the AIS must be decomposed into identifiable, understandable, manageable, and traceable units known as configuration items. Traceability extends from the initial system baseline through the system's entire life cycle. Once something is designated a configuration item early in the system's development, every change must be under CM control.

***CONFIGURATION ITEM IDENTIFICATION***

***The smallest identifiable and understandable items in the system that can be changed and that might have an effect on the system's operation or security profile is considered a configuration item.***

A configuration item represents the portion of system subject to independent configuration management control procedures. The smallest item in the system that can be changed and that might have an effect on the system's operation or security profile is considered a configuration item. Not only is the hardware and software in the system controlled, but also the design, user documentation, and system tests are under control.

The following list represents common system components decomposed into configuration items:

1) Software and firmware components of the baseline design.
2) Any changes to the TCB hardware, software, and firmware since the previous baseline.
3) Design and user documentation.
4) Software tests including functional and system integrity tests and associated documentation.
5) Development tools including any configuration management tools.
6) Any tools used for generating current configuration items.
7) Any audit trail reduction tools used in the configuration management context.
8) Maintenance guidelines
9) Any other components of the AIS as broadly defined.

Each configuration item is individually indicated by a unique identifier, plus information related to the item's effect on the system. This information is contained in the Configuration Management Plan for the AIS. When alterations or additions to the existing configuration occur, a new unique identifier is assigned. Identifiers are assigned early in the design of a system to ensure traceability of each new configuration change over its life cycle.

It is important to select configuration item components that are appropriate for the systems size. Many small components will overwhelm the system auditors while too large of components will require considerable identification data.

***CONFIGURATION CONTROL***

***CC covers the evaluation, coordination, and approval/disapproval of a proposed change.***

***Attempts to control the system configuration as it was initially designed and specified in the design documents.***

***The CM Plan is a simple description of what is to be done to implement CM in the AIS.***

***Changes are implemented through an Engineering Change Order (ECO).***

## Configuration Control

Configuration control involves the evaluation, coordination, and approval/disapproval of a proposed change. If a particular change is approved and later identified as a problem, the traceability control function allows for re-configuring to the previous state.

The initial aim of configuration control is to control the system configuration as it was initially designed and specified in the design documents. The Configuration Management Plan is a simple description of what is to be done to implement configuration management in the AIS. The document is flexible and intended to be upgraded as additional needs are placed on the system.

Since configuration control applies to both baseline design and changes, it must also address formal policies and procedures for correcting any security problems identified in a system or product. Changes are normally implemented through an Engineering Change Order (ECO). Note that changes to software sometimes aren't completely reflected in an ECO. A general format for ECO's is provided below:

1) The ECO provides an orderly mechanism to propagate change across the system and assure synchronization, connectivity, and continuity of alterations.
2) The preparation of ECO's is under Configuration Change Board control.
3) No system change of any kind can occur without direction by an ECO.

***CONFIGURATION CONTROL PROGRAM (CCP)***

***Provides for constant checking and approval of changes.***

***Control implemented at the individual AIS level and at each site for multiple AISs.***

***Mechanism must be in place to ensure each site receives the same version of the system and that no single AIS can act to compromise the entire system.***

***Control is especially important when different contractors are used to provide maintenance.***

4) Each ECO retains the identities of the initiating Service Improvement Request (SIR) or other related SIR's or ECO's.

5) ECO's are retained as evidence of formal change review and approval.

When any subsequent configuration item changes are made to the AIS, not only must each change be formally approved by the controlling party, but the Configuration Management Plan and all related material must also be upgraded to ensure complete auditability.

A configuration control program should provide for constant checking and approval of changes. Control is implemented at the individual AIS level and at each site when multiple AISs are used. The mechanism must be in place to ensure each site receives the same version of the system and that no single AIS can act to compromise the integrity of the entire system. This control is especially important when different contractors are used to provide maintenance to controlled equipment.

**Configuration Control Board (CCB)**

Configuration control functions are flexible and do not necessarily required a formal control board for their implementation. The TCSEC requires a formal board of qualified individuals be established for Class B2 and above. The CCB should include members representing the following areas:

- Program Management
- System Engineering
- Quality Assurance
- Technical Support
- Integration and Test
- System Installation
- Technical Installation
- Hardware and Software/Firmware Acquisition
- Program Development
- Security Engineering
- User Groups

***CONFIGURATION STATUS ACCOUNTING***

***The mechanism by which progress on developing systems is reported.***

***Objective is to record and report on all CM information significant to system security.***

***Procedures enable logistics support such as instruction manuals and maintenance histories.***

**Configuration Status Accounting**

Configuration status accounting is the mechanism by which progress on developing systems is reported. Establishment of a new baseline or meeting a design milestone are examples of what should be recorded as configuration status accounting information. Its objective is to record and report on all configuration management information of significance to the security of the system. Data recording, storing, and reporting are the primary means of accomplishing this task. Nearly any format for recording this information is acceptable, including on-line data bases.

The accounting procedures enable logistics support such as instruction manuals and maintenance histories to be developed. Sufficient information should be available that a complete history of any

AIS can

### Configuration Audit

The configuration audit involves checking that the configuration accounting information is complete. Proposed changes are reviewed and audited for their effect on the entire system. Changes include both review and testing. The audit minimizes the likelihood that a particular change will be implemented without formal review.

The configuration audit should verify that:

- The architectural design satisfies the requirements,
- The detailed design satisfies the architectural design,
- The software code implements the detailed design,
- The item/product performs per the requirements,
- The configuration documentation,
- The item/product match

Both hardware design and software code audits follow roughly the same review and formal audit procedures.

### Baselines

When a product is under development, baselines are established at pre-selected design points in the system life-cycle. Baselines are defined corresponding to major design or life-cycle milestones, normally established by the Configuration Control Board. Each baseline serves as a cutoff point or completion point for one segment of the development process. The characteristics common to all baselines are that the design of the system is approved to that point and that any future changes to the design will impact the system.

The initial baseline established is the functional baseline. It is derived from the requirements documentation which lists performance criteria. The final baseline, the product baseline, contains the finished version of the system that is turned over to integration testing or other end item testing. This baseline documents the version of the system at the end of the development phase and nearing final release.

### Equipment Repair and RCM (Both COTS and GOTS)

For all equipment, certain maintainability principles apply during its life cycle. Maintainability Engineering is intended to guide initial equipment designers in optimizing maintainability requirements, reliability, and logistics effectiveness by taking into consideration the support and maintenance of a system. Maintenance Engineering includes maintenance procedures, maintenance instructions, maintenance task analysis, and resource requirements in personnel, equipment, and facilities to conduct a Logistics Support Analysis.

Reliability Centered Maintenance (RCM) is a method for developing maintenance programs utilizing analytical methods to determine the amount of maintenance and optimum distribution of tasks which are essential to preserving the inherent safety, reliability, and security of the system, consistent with the lowest life-cycle cost.

A formal RCM process can be developed for most programs. One important aspect of this approach is breaking the system into discrete indenture levels to facilitate management of the analysis, upgrade, or maintenance program. The breakdown resembles the SSEM levels used by the Air Force. This type of breakdown can provide the basis for assessing impacts, including security impacts whenever equipment is evaluated for maintenance, upgrade, or repair.

An analysis of equipment reliability, in large part, should drive the decision about the work content of an RCM program. For a classified processing system, security rather than long-term reliability becomes the driving requirement.

For a TEMPEST AIS, if the repair or upgrade is not a critical feature, such as installing a larger hard disk or more RAM, it can normally be added without an extensive RCM process in place and without any additional TEMPEST testing. If a commercial, discrete component or particular electronic circuit package is required to repair an AIS, this new part can be used without a TEMPEST or AIS re-test so long as it has the same specified value or the same logic family. In either case, a formal RCM process would be beneficial for tracking purposes, since the repair information must be maintained in a configuration management program of some type.

**Vulnerability Survey**

A risk analysis is required for every AIS to meet C2 functionality as described in DoDD 5200.28. These risk assessments do not cover in detail the emission requirements for TEMPEST type equipment. For this equipment, some relaxation of emission requirements is allowable based on if the equipment is to be used inside or outside the United States. Regardless of emission level acceptable, one of the following measures is required for acceptance of formal TEMPEST equipment. An Equipment TEMPEST Radiation Zone (ETRZ) must be established, a vulnerability study is preformed, or each item of equipment must be TEMPEST-compliant.

Establishing an ETRZ, or performing a zone test on a facility, is simple when equipment is to used in one general location. The limitations are that the TEMPEST profile of each item of equipment must be known, and the equipment is only acceptable so long as it is located in an area where the zone limitations are also known.

One simple method of establishing an ETRZ with non-TEMPEST commercial equipment is to assume that all emissions from the particular equipment are compromising. Since COTS equipment meets Federal Communication Commission (FCC) emission limits, its maximum radiated emission profile can be predicted. The difference between the FCC limits and the relevant TEMPEST limits establishes the amount of attenuation (or space loss) necessary to be TEMPEST-compliant within a zone. Although acceptable and sometimes used, this type on an analysis should only be undertaken by an individual experienced in this technique.

An inexpensive TEMPEST quick-scan of modified equipment is acceptable in a vulnerability analysis when upgrade or modification changes affect critical items, depending on which items are modified and how. It is beyond the scope of this document to define the exact conditions of usage and criteria whereby scan information is allowed.

In most cases tactical equipment is initially TEMPEST-compliant. Any modification which employs COTS equipment must be evaluated by one of the three methods specified. Approval to use equipment that is less than full TEMPEST-compliant is the responsibility of the Certified

TEMPEST Authority for the service or organization involved. In the continental US, TEMPEST equipment does not need to meet the same standards as is equipment used outside the U.S.

### Continuing Life-Cycle through Decommissioning

Once the product has been delivered and deployed, continuing dialog with the customer is necessary to solicit feedback and identify software bugs or vulnerabilities that are identified, plus learn of new capabilities that may be useful to implement. This dialog may also identify capabilities that other products can provide.

As with all lifecycles, the stages of TLC consist of requirements gathering, design and development, quality assurance testing, distribution, software change and configuration, and maintenance are all part of the application lifecycle, as is decommissioning.

### Conclusions

Configuration Management is an essential part of every AIS. The programs complexity depends on how the AIS is defined. Since an AIS may consist of many computers and peripherals of various sizes working together in support of a single function, this "single function" theory forms the basis of defining AIS boundaries. Computer systems that share their functionality are identified as self-contained AIS. From either perspective, formal configuration management controls have been imposed.

Successful configuration management is built around four main objectives: control, identification, accounting, and auditing. It is a requirement for trusted systems in classes B2 and above. However, a CM system should be in place for all systems regardless of class ratings or trust requirement.

Configuration management supports the engineering practices, operational objectives, and security requirements of an overall quality assurance program. Configuration management must also be considered a vital element of the AIS security posture. However, it is not strictly a security control and traceability tool. It has historically been specified as part of operational documents. The CM documentation should be an ongoing process accurately reflecting the entire system at all times. No changes to the system should be performed, including upgrades and ad-hock procedures, without documenting those changes in the configuration document.

***CM CONCLUSIONS***

***Configuration Management is an essential part of every AIS, regardless of the level of trust imposed.***

***The programs complexity depends on how the AIS is defined. Since an AIS may consist of many computers working together in support of a single function, this "single function" theory forms the basis of defining AIS boundaries, hence CM requirements.***

***CM is built around four main objectives: control, identification, accounting, and auditing.***

Configuration management should be included as an overall philosophy, not just a policy. The documentation necessary to support the CM philosophy is the configuration documentation. It should contain the initial system configuration as installed and operational. This is considered the "base line."

The configuration management documentation and other appropriate system security documentation must be maintained by the appropriate personnel. Proposed changes to the system should be placed before a configuration panel. This panel, composed of systems, applications, users, and security experts, will evaluate each proposed change for its impact on the system. The panel will then determine whether to grant the new configuration request.

An effective configuration management system should accurately document what was required to be built, what was built, and what is presently being built.

## Appendix A

## Organizational Requirements

***CM REQUIREMENT DOCUMENTS***

***Most, but not all CM requirements for defense organizations evolved from the Trusted Computer System Evaluation Criteria (DOD 5200.28-STD).***

***COMSEC CM requirements, TEMPEST requirements, and SCIF installation requirements evolved from other sources.***

***Currently the various Government organizations have generated individual requirements to cover their own needs.***

### NCSC-TG-006 Version-1, A Guide to Understanding Configuration Management in Trusted Systems

This is the primary configuration management document of the "Rainbow Series." As discussed in Section 5.2.5.1, the document applies primarily to software-type controls rather than hardware controls of trusted computer bases (TCBs). The following information is applied to class A1 systems. Class B2 systems apply Requirements 1 through 11. Class B3 system requirements are listed as the same as B2 systems. However, since class B3 systems require more documentation, this means that the additional documentation will be maintained under the CM program.

### Class A1 Trusted Systems

Configuration Management Requirements:

1. During development and maintenance of the TCB, a configuration management system shall be in place.

2. The configuration management system shall maintain "control of changes to the descriptive top-level specification (DTLS)."

3. The configuration management system shall maintain control of changes to "other design data."

***DOD 5200.28-STD, CSC-STD-001-83***

***DOD TRUSTED COMPUTER SYSTEM***

***EVALUATION CRITERIA***

***Addresses security requirements for ADP systems acquisitions.***

***1) specific security feature requirements***

***2) assurance requirements***

4. The configuration management system shall maintain control of changes to "implementation documentation."

5. The configuration management system shall maintain control of changes to the "source code."

6. The configuration management system shall maintain control of changes to "the running version of the object code."

7. The configuration management system shall maintain control of changes to "test fixtures."

8. The configuration management system shall maintain control of changes to test "documentation."

9. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB.

10. The configuration management system shall provide tools "for generation of a new version of the TCB from the source code."

11. The configuration management system shall provide "tools for comparisons of a newly generated TCB version with the previous version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB."

12. During the entire life cycle, i.e., during the design, development, and maintenance of the TCB, a configuration management system shall be in place for all security-relevant hardware, firmware, and software.

13. The configuration management system shall maintain control of changes to the TCB hardware.

14. The configuration management system shall maintain control of changes to the TCB software.

15. The configuration management system shall maintain control of changes to the TCB firmware.

16. The configuration management system shall maintain control of changes to the formal model.

17. The configuration management system shall maintain control of changes to the formal top-level specifications.

18. The tools available for configuration management shall be maintained under strict configuration control.

19. A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy or copies of all material used to generate the TCB.

### DOD 5200.28-STD, CSC-STD-001-83, DoD Trusted Computer System Evaluation Criteria, 15 August 83

There are two distinct sets of security requirements for ADP systems acquisitions. These requirements are: 1) specific security feature requirements, and 2) assurance requirements. Assurance requirements apply to systems that cover the full range of computing environments from dedicated controllers to full-range multilevel secure resource-sharing systems. Assurance provisions from DoDD 5200.28 were previously discussed for Navy applications in Section 4.0.

### 5200.28 Configuration Management Sections

Configuration management is one of the assurance control and evaluation criteria specified in DoDS 5200.28. As stated in Section 3.0, these criteria provide a basis for the evaluation of the effectiveness of trusted security controls (primarily software) built into ADP system products. However, no formal configuration management requirements are called out for trusted systems below the level of B2. The following discussion describes the formal CM requirements for classes B2 and above.

Configuration management is required at the B2, B3, and A1 processing levels. The requirements at the B2 and B3 levels are identical; the requirements at the A1 level are more stringent. The requirements are provided below:

a. Classes B2 and B3 - Structured Protection:

"Life-Cycle Assurance - Configuration Management

"During development and maintenance of the TCB, a configuration management system shall be in place that maintains control of changes to the descriptive top-level specification, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB."

b. Class A1 - Verified Design:

Life-Cycle Assurance - Configuration Management

Class A1 provisions include the previous requirements plus the additional requirements indicated in bold. "During the entire life cycle, **i.e. during the design, development,** and maintenance of the TCB, a configuration management system shall be in place **for all security-relevant hardware, firmware, and software** that maintains control of changes to **the formal model,** the descriptive **and formal** top-level **specifications**, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools, **maintained under strict configuration control**, for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. **A combination of technical, physical, and procedural safeguards shall be used to protect from unauthorized modification or destruction the master copy of copies of all material used to generate the TCB.**"

Since most Department of Defense AIS are required to meet C2 functionality, the CM requirement of DoDS 5200.28 does not formally apply. What generally occurs at the organization level is that provisions for hardware CM are provided based on an interpretation of other documents. The requirements of these documents are applied directly to the equipment as used in specific applications. For software-related CM that may be applied at the C2 level, the interpretation is generally based on the general life-cycle assurance provisions of class C2 under DoDS 5200.28.

### How the Navy Performs Configuration Management (CM)

Software-related CM information is widely distributed. However, formal hardware-related CM information is not readily available from most organizations. The Navy has an extensive CM program and will be the focus of this section.

In the Navy's "AIS Security Manual", the Navy applies configuration management as a quality-assurance function. These requirements are taken directly from DoDD 5200.28. One of the control objectives of configuration management is to assure that the security policy has been implemented correctly by a particular AIS, and that the system's protection-relevant elements accurately enforce the intent of that policy. This assurance must include a guarantee that the trusted portion of the system works only as intended.

To accomplish these objectives, the AIS Security Manual specifies that two types of assurance are needed: "They are life-cycle assurance and operational assurance. Life-cycle assurance refers to steps taken by an organization to ensure that the system is designed, developed, and maintained using formalized and rigorous controls and standards. Computer systems that process and store sensitive or classified information depend on the hardware and software to protect that information. It follows that the hardware and software themselves must be protected against unauthorized changes that could cause protection mechanisms to malfunction or be bypassed completely."

Reevaluation is necessary whenever changes are made that could affect the integrity of the protection mechanisms. The Navy feels that the hardware and software interpretation of the security policy will remain accurate and undistorted.

### Navy Assurance Control Objectives

The AIS Security Manual states that: "While life-cycle assurance is concerned with procedures for managing system design, development, and maintenance; operational assurance focuses on features and system architecture used to ensure that the security policy is enforced without circumvention during system operation. That is, the security policy must be integrated into the hardware and software protection features of the system."

"Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life-cycle."

### Navy CM for Workstations and AIS Terminals

The Navy has developed an extensive configuration management program, based on the requirements of DoDD 5200.28. Included below is the relevant text from Chapter 26 of the Navy's AIS Security Manual.

"26.1 General. Configuration Management is that part of security concerned with the management of changes made to an Automated Information System (AIS) throughout the development and operational life of the system. Configuration Management protects a system against unauthorized modifications and ensures that all the properties of a system are maintained after an authorized modification. Configuration Management provides both control and accountability for all modifications made to a system.  Configuration Management also provides assurance that changes made to a classified system do not compromise the original classification of the system."

"26.1.1  Objective.  This Chapter should provide all personnel in AIS environments with enough information concerning configuration management to identify those who are responsible for configuration management of AISs.  It will also help determine where configuration management should be practiced, when configuration management should be implemented, and why configuration management is an important AIS security procedure."

***NAVY CM FOR TERMINALS & WORKSTATIONS***

***CM is that part of security concerned with the management of changes made to an AIS throughout the development and operational life cycle.***

***CM protects against unauthorized modifications.***

***CM provides both control of potential compromises and accountability for changes made.***

"26.2  Roles and Responsibilities.  The overall responsibility to identify, control, and monitor the computer system's configuration posture is shared between the Automated Data Processing Security Officer (ADPSO), the Automated Data Processing System Security Officer (ADPSSO), and the AIS users."

"26.2.1  ADP Security Officer (ADPSO).  The ADPSO will:

"a.  Provide policy guidance and interpretation of DOD/DON policies concerning Configuration Management."

"b.  Identify written procedures for requesting changes to an AIS's configuration."

"c.  Assist in the analysis of the system configuration and processes to determine the correct classification of the system."

"d.  Monitor changes to the system configuration to ensure that the system is classified correctly and that the appropriate security measures are incorporated in the system design."

"26.2.2  ADP System Security Officer (ADPSSO).  The ADPSSO will:

"a. Identify the type of user awareness training needed to  protect the integrity of the AIS."

"b.  Maintain a terminal/microcomputer locator list."

"c.  Track the movement of terminals/microcomputers within the AIS configuration."

"d.  In a large-scale AIS environment, review the system specification to ensure that the appropriate security measures are intact."

"e. In a large-scale AIS environment, ensure that the system integrity is maintained by verifying that only the System Administrator or an authorized person has the capability to make changes to the system."

"f.  Ensure that configuration management is in place and conforms to the established policies identified by the ADPSO."

"g.  Identify the hardware and software/firmware in the AIS configuration."

"h.  Receive and review all change requests to the AIS configuration."

"i.  Document and report all changes, especially those effecting AIS users."

"j.  Verify that changes made to the AIS configuration are functionally correct by testing the AIS processes."

"26.2.3  High-Level AIS Environment.  In high-level AIS environments where large scale AISs such as mainframes are used, a Configuration Control Board should be established.  This Board normally consists of the key personnel who are responsible for programming, software testing, hardware  maintenance, and technical support of the AISs."

"26.2.4  Configuration Control Board (CCB).  The CCB should  consist of the following members who are jointly responsible for:

"a.  Scheduling meetings to discuss Configuration Management topics such as proposed changes, configuration status, accounting reports, and other topics that may be of interest to the different areas of the  system  development."

"b.  Prioritizing the approved modifications to the AISs to ensure that those system modifications that are most important are implemented first."

"c.  Verifying that only the approved modifications have been incorporated into the AIS once changes have been completed."

"26.2.5.1  System Administrator.  The System Administrator  is  responsible for monitoring and controlling the system configuration.  The System Administrator is also considered the Program Manager.  He/she will assist in the analysis and review of the requested modifications of the system design.  The System Administrator should be the only person with system permission to modify the system design after authorization has been granted by the CCB.

"26.2.5.2  System Programmer.  When directed by the System Administrator, the System Programmer is responsible for making approved software changes.  The System Programmer should also be able to perform emergency software fixes and changes when required.

"26.2.5.3  Integration and Quality Assurance Personnel.  The Integration and Quality Assurance Personnel are responsible for loading and testing all AIS software.

"26.2.5.4  System Engineer.  The System Engineer is responsible for ensuring that the AIS is functioning at normal capacity.  The System Engineer can provide valuable recommendations and opinions on proposed changes to the AIS.

"26.2.5.5  Security Engineer.  The Security Engineer is responsible for putting in place the security measures necessary to meet the security requirements associated with the highest classification of the information processed on the AIS.  The Security Engineer will also provide recommendations and comments on the security impact of the proposed changes to the AIS.

"26.2.5.6  Hardware and Software/Firmware Supply Officer.  The Hardware and Software/Firmware Supply Officer can best determine if there is a product available that will provide the capability identified in the change request.  Commercial items which meet government standards may be purchased if they are approved by the CCB.

"26.2.5.7  Technical Support Personnel.  Technical Support Personnel consist of representatives from the remaining technical support areas of the AIS environment.  These representatives will assist in the analysis of the requested changes, especially if the changes will impact their area of expertise.  Their contributions will ensure that unnecessary and contradictory changes are prevented.

"26.2.5.8 Technical Librarian.  The Technical Librarian will maintain an up-to-date accounting of all changes to technical documentation maintained in the Technical Library.  The Technical Librarian will furnish copies of appropriate documentation to the System Programmer to assist them in the system analysis and modification.

"26.2.5.9  AIS User Group.  The AIS users will normally submit the AIS change request.  When requested changes are submitted from someone other than the system user, the system user should review the request to ensure that the change would enhance and not hamper the system's performance.  The AIS user should:

"a.  Notify the ADPSSO when an unannounced change to the AIS configuration is detected or when the system fails to do what it is intended to do."

"b.  Propose modifications/enhancements to the AIS system."

"c.  Test the system's performance after a modification has been completed."

"d.  Practice the recommended security safeguards to protect the integrity of the AIS."

"26.3  Procedures.  Configuration Management consists primarily of four separate tasks: identification, control, status accounting, and auditing.  For every change to the AIS, these four tasks should be carried out.

"26.3.1  Configuration Identification.  The first step in Configuration Management is to identify the configuration of the system.  The basic function of configuration identification is:

"a.  To identify the components of the system design."

"b.  To use, in high level AIS environments, configuration items and baselines to accurately identify the configuration of the system throughout the system's life-cycle."

"26.3.1.1  Configuration Items.  Configuration Item is the unique subset of the system configuration that represents the smallest portion of the system."

"26.3.1.2  Configuration Baselines.  The Baseline concept is a technique used to identify the system configuration.  A baseline should identify a specific version of a system or major milestones in the system's development.  There are three types of baselines:

"1.  Functional Baseline;

"2.  Allocated Baseline;

"3.  Product Baseline.

"26.3.1.2.1  Functional Baseline.  The Functional Baseline is established at the system level.  It is based on documented user-defined system requirements.  Once the functional baseline is established, any modifications made should be approved by the CCB.

"26.3.1.2.2 Allocated Baseline. The Allocated Baseline will be established after the analysis of the system requirements. This baseline identifies all of the required functions with a specific configuration item which is responsible for the function.

"26.3.1.2.3 Product Baseline. The Product Baseline should contain that version of the system that will be turned over for integration testing. This baseline signifies the end of the development phase and should contain a releasable version of the system.

***NAVY CONFIGURATION BASELENES***

***The Baseline concept is a technique used to identify the system configuration.***

***A baseline should identify a specific version of a system or major milestones in the system's development.***

***Navy defines Functional Baselines, Allocated Baselines, and Product Baselines.***

"26.3.2 Configuration Control. Configuration Control should be practiced throughout the system's life-cycle. It requires controlling every change to the system documentation, hardware, and software/firmware by thoroughly reviewing and analyzing all requested changes before disapproving or authorizing those changes.

"26.3.3 Configuration Status Accounting. After the components of the system have been identified, Configuration Status Accounting should be used to record and report on the configuration of the system throughout all changes.

26.3.4 Configuration Audit. The final requirement is that the system configuration be audited to verify that the completed changes are functionally correct and consistent with the security policy of the system.

26.3.5 Configuration Management Plan. In order to successfully manage an AIS configuration, a well thought-out plan should be prepared immediately after project initiation. The Configuration Management Plan should:

"a. Define how the configuration management will be implemented as it relates to the identification, control, accounting, and auditing tasks.

***THE CM PLAN***

***Define how CM configuration management will be implemented, individual responsibilities, change procedures, and ensures life-cycle support of security features.***

"b. Define the roles played by the system designers, system developers, management, security staff, and the Configuration Control Board.

"c. Define the procedures to be followed during configuration management.

"d. Define any existing emergency procedures; for example, procedures for performing a time-sensitive change.

"e. Ensure that the security features and assurances supported by the Plan are still maintained after the change."

***AIR FORCE SSEM CM***

***SSEM imposes security oriented configuration management, through the implementation of appropriate security requirements, on all related functions and devices within the life cycle of a program.***

## Air Force System Security Engineering Management

The U.S. Air Force has implemented MIL-STD 1785[2] in an attempt to provide overall control of security-related functions within the total acquisition process. System Security Engineering Management (SSEM) is an element of systems engineering that applies scientific and engineering principles to identify and reduce overall security vulnerabilities from all INFOSEC functions. SSEM can be applied at all levels of complexity from box design to network control to enhance quality assurance. In essence, SSEM imposes security oriented configuration management, through the implementation of appropriate security requirements, on all related functions and devices within the life cycle of a program.

## Specified Minimum Hardware CM Needed to Maintain Security

This section addresses hardware-related configuration management information. It describes the relevant technologies and applicable requirements documentation used to measure or control these technologies.

## Applicable Technologies

Information security (INFOSEC) is an all-encompassing term used to describe all measures intended to prevent unauthorized access to or distribution of classified information. It is composed of three principal components: emission security (TEMPEST), computer security (COMPUSEC), and communications security (COMSEC). All three INFOSEC components play a direct role in the network's protection, along with other components. While each component has a unique meaning, some of these meanings may be unclear and overlap in the modern computer network-based communication age.

***INFOSEC***

***INFOSEC is an all-encompassing term used to describe all measures intended to prevent unauthorized access to or distribution of classified information.***

***It is composed of three principal components: emission security (TEMPEST), computer security (COMPUSEC), and communications security (COMSEC).***

COMPUSEC means protective (usually software) measures to prevent the unauthorized access to or use of automated data processing (computer-based) information. COMSEC or communications security means measures taken to deny unauthorized persons access to telecommunications information. This usually involves a proper isolation between RED (non-

[2] MIL-STD 1785, Systems Security Engineering Program Requirements, as implemented by AFR 207-1, 3 October 1988.

protected) and BLACK (protected) information.  TEMPEST relates to compromising emanations that may radiate from equipment.

The configuration management of the Worldwide Military Command and Control System (WWMCCS) Intercomputing Network (WIN) is useful to investigate since it is under the control of the Joint Staff and must interface with all other service branches. For a classified network like the WIN, TEMPEST-secure computers are interconnected through a telecommunications device and have administrative controls to protect against unauthorized network entry.

The current configuration management and security requirements imposed on equipment used for the WIN in all applications are under the control of the Joint Staff.  Joint Pub 6-03.7 is the primary governing document for this equipment.  The current equipment has been identified as networked and stand-alone TEMPEST-approved automated information systems (AISs).  The WIN is a network of mainframes, minis, and micros that operate in a system-high security mode.  As such, all features of the system, including output products and storage media, are classified at the TOP SECRET level.  These systems are "intelligent," requiring safeguards at both the workstation level, and at the system-interconnect level.

WIN computer workstations are used in a classified processing environment.  WWMCCS is a "B1-like" system but has not been submitted to the formal evaluation process.  All WIN equipment is required to meet C2 functionality as a level of trust.

At the workstation level, the minimum level of trust required by the Joint Staff is that of "class C2 functionality."  The Navy has also defined a level of C2 functionality that is acceptable for its systems.  DoDS 5200.28 has no trusted computer (software) configuration management requirements called out for this class but implies that both hardware and software CM "should be" implemented at lower levels of trust.  C2-level trusted systems have primarily software and procedural safeguards, as opposed to hardware TEMPEST or COMSEC controls.  This means the configuration management controls on the WIN are not directly traceable to DoDS 5200.28 but to other requirement documents.  The TEMPEST controls on the WIN stem directly from its processing of TOP SECRET data, while its COMSEC and RED/BLACK controls relate directly to its network interconnect conditions. Interconnect will be addressed further in Section 6.0 under policy requirements and in 6.1 related to AIS boundaries.

***JOINT STAFF CM***

***The WWMCCS Intercomputer Network (WIN) is a joint resource used by the U.S. Armed Forces.***

***The Joint Staff has the requirement to integrate ist WWMCCS equipment with all other DOD organizations.***

***WWMCCS equipment is primarily specified as TEMPEST AIS at the C2 or higher and COMSEC equipment.***

***For WIN workstations, the minimum level of trust required by the Joint Staff is "class C2 functionality."***

### Specification Documents (Joint Pub 6-03.7)

The WWMCCS Intercomputer Network is a joint resource used by the Armed Forces of the United States.  Therefore, security for the WIN falls under the responsibility of the Joint Staff.  This organization has published policy documents which provide up-to-date guidance on all aspects of security for the WIN. Joint Pub 6-03.7 is the security policy requirements document governing the WIN.  The document is referenced many times in this study in addition to the brief information provided below.

Network security architecture is covered in Section III-5 of Joint Pub 6-03.7. Among the requirements listed in this section are those regarding LAN to WIN, LAN to LAN, as well as the specific reference to LAN equipment meeting the C2 functionality requirement. Section III-5 also refers to NCSC-TG-011, Trusted Network Interpretation Environments Guidelines (Rainbow Series), as the evaluation document against which Joint Staff functional security architecture has been developed.

Accreditation requirements are defined in Section V-1 of Joint Pub 6-03.7. Section 5-1.d states, "Each WIN multi-user host and connecting AIS (RNPs, LANs, etc.) will be accredited for stand-alone operations. Furthermore, each WIN multi-user host will be accredited to operate in the WIN; i.e., the host's connection to the WIN will be accredited by the WIN DAA." A DAA is a Designated Approving Authority.

Other documents relate to the Joint Staff requirements but do not necessarily require conformance. This study focuses not only on the Joint Staff requirements for CM (currently under revision) but also on the requirements for certain equipment types based on their applications and capabilities.

## MCO P5510.14, ADP Security Program for Marine Corps

The Marine Corps ADP Security manual provides technical direction and guidance governing the security of Marine Corps ADP activities. Three parts of this document are relevant to this study: Section 2007, Host and Remote Terminals; Section 5001, Information (Communications Security); and Sections 6002 through 6004, Emanations Security. The relevant material from this document is provided below and provides the legal basis for subsequent interpretations provided for Marine Corps/WIN applications.

***MARINE CORPS REQUIREMENTS***

***Marine Corps requirements are similar to other service requirements except that they must address tactical and interconnect concerns much closer.***

***Tactical equipment types have significant COMSEC, TEMPEST, and maintenance concerns.***

Section 2007, Host and Remote Terminals:

"1. Increasing reliance upon remote terminal devices generally represents a significant increase in overall ADP system vulnerability. Protection of systems operating under these conditions requires careful delineation of responsibilities and procedural agreement between host computer and remote terminal user organizations.

"a. Security characteristics of remote terminals and interface devices, if required, as well as security measures for the areas in which they are located, will be prescribed by the activity having security responsibility for the main or host computer.

"b. Remote terminal user organizations will be responsible for ensuring conformance with approved security measures and compliance with security procedures.

"c.  Measures and procedures required to ensure overall system integrity will be agreed upon before remote terminals and other supporting devices are connected to the main computer.

"2.  When one or more ADP activities join to participate in network operations, a network or security officer shall be designated for the network by the sponsor.  This officer will ensure full implementation of necessary security procedures.  As with other remote operations, joint agreement shall be reached and formal procedures established prior to internetting.  The network security officer shall prescribe security requirements, protocols, and standards for the system, while individual site managers will ensure their adherence and enforcement."

Section 5001, Information:

"Security policy requires that all telecommunications be separated into two categories:  classified and unclassified communications.  All communications circuits employed to interconnect remotely located components of Marine Corps automation systems or networks which process or store classified information will be provided COMSEC.  Appropriate COMSEC will be achieved by use of standard military encryption systems produced by the National Security Agency (NSA), installed in accordance with the provisions of Military Handbook (MIL-HDBK 232) or Protected Wireline Distribution System (PWDS) or Intrusion Resistant Cables.  PWDS circuits will be installed as prescribed by MIL-HDBK 232.  These circuits are costly and suitable for only short-distance communication (normally within a single building or facility, which is under continuous physical/personnel security controls and approved methods of user-authentication."

Chapter 6 - Emanations Security

Section 6002, Information:

"The presence of compromising emanations depends upon the type of equipment used to process the information; the method of installation; and the maintenance status of the  equipment. COMNAVSECGRU carries out the compromising emanations (TEMPEST) control program for the Marine Corps.  TEMPEST support takes three forms:  non-instrumented TEMPEST inspections, instrumented TEMPEST tests, and technical advice and assistance."

Section 6003, Responsibilities:

"1.  The responsibility of an accreditation authority is to:

"a. Ensure that the duties and responsibilities are fulfilled  by commanders of ADP activities under their jurisdiction at both headquarters and subordinate levels."

"b.  Ensure that TEMPEST technical assistance is provided from supporting elements during the engineering planning and installation phases of new or reconfigured ADP activities."

"c. Ensure that contractual documents for those contracts involving the use of ADP activities to process national defense information include appropriate TEMPEST provisions.  CMC (Code CCT)  will provide advice and assistance, as requested, in formulating contractual TEMPEST provisions."

Section 6004, TEMPEST Tests:

"1. There are basically three methods recommended for controlling compromising emanations:

"a.  To provide the equipment with a physical control zone (PCZ) of sufficient spherical diameter to preclude successful hostile intercept action."

"b. To implement minimum essential countermeasures to contain  compromising signals within the accepted PCZ."

"c. To design or identify the equipment to limit the strength  of  compromising signal to acceptable limits within the available PCZ.  To decide which of the foregoing is necessary, the equipment must be tested.  If the equipment has not been previously tested, it may be tested by having an onsite survey conducted by COMNAVSECGRU personnel."

2. A PCZ does not automatically require a fenced, guarded area or closed-circuit surveillance system.  Only under the most unusual circumstances will that action be necessary purely for TEMPEST authority."

**IRM-5239.08, Computer Security Procedures, U.S. Marine Corps**

This document references MCO P5510.14 and provides additional guidance and amplification of the requirements specified in the basic ADP security documents.  It is published under the authority of MCO 5271.1.  Of importance in this document is Chapter 11, Network Security; paragraph 11.3.1, Interservice and Interagency Networks.  This paragraph is provided below:

"Organizations that depend on interservice or interagency networks should develop a Memorandum or Agreement (MOA) for each AIS networked with another service or agency system and forward it to each command, service, or agency DAA for review and mutual acceptance."

## 6.4 Classified and Unclassified Documents Related to TEMPEST Security

There are several requirement documents, some not readily available, that deal with most aspects of TEMPEST configuration management.  The following sections describe relevant information from the most commonly used documents.

### 6.4.1 NSTISSIM Series

The NSTISSIM documents are issued by the National Security Agency (NSA) to provide requirements for accrediting TEMPEST equipment.  Only one document of the NSTISSIM series, NSTISSIM TEMPEST/3/91, Maintenance and Disposition of TEMPEST Equipment, deals with configuration management functions of TEMPEST equipment. This document only defines some minimum maintenance responsibilities, and provides no detailed guidelines.  In this document, TEMPEST equipment is defined as equipment listed on:  the Endorsed TEMPEST Products List (ETPL), Preferred Products List (PPL); the NATO Recommended Products List (NRPL); and equipment that complies with either Level I or II of NSTISSIM TEMPEST/1-91.

Under user responsibility, item 7a, "The user must ensure that data resident on the equipment is not compromised during the maintenance/disposition process."  Item 7d says "A TEMPEST equipment log must be maintained that includes date of maintenance, action taken, technician name, model, and serial number.  Recertification testing after maintenance is left to the discretion of the department or agency responsible."

### 6.4.2 Technical Security Requirements Document (TSRD)

***TEMPEST CM***

***DOD TEMPEST equipment CM requirements are normally defined in equipment specifications.***

***Commercial TEMPEST equipment only have the CM guidelines imposed under quality assurance provisions of the TSRD.***

TSRD procedures and specifications covering the design and controls for TEMPEST and COMSEC programs are specified by the National Security Agency. TSRD No. 88-9B identifies the management, design and test requirements placed on TEMPEST equipment to be listed through the TEMPEST Endorsed Products Program. This document also offers some additional guidelines related to configuration management of TEMPEST equipment.

The following information provides clarification and guidance regarding the life-cycle, quality assurance, upgrade, and maintenance characteristics of TEMPEST equipment. These requirements are imposed on the manufacturer, but several also apply to the user once the equipment becomes his responsibility. In the document, they primarily fall under the requirements of the quality assurance program.

Manufacturers must designate a Company Appointed TEMPEST Authority (CATA) to be responsible for developing and maintaining an NSA approved QA program for each product tested and approved for inclusion on the Endorsed TEMPEST Products List (ETPL). Of primary importance in this program is the Critical Features List. No engineering change can be made to a ETPL product without written approval from the CATA. However, only changes to items on the Critical Features List require re-testing in most instances. The following information lists the requirements imposed on the baseline TEMPEST equipment for insuring product integrity.

The CM and control system includes:

Critical Features List - Parts, Assemblies, Procedures, and Manufacturing Processes

Configuration Baseline - Drawings, Lists of Components, and Ancillaries

Initial Physical Configuration Audit (PCA), Plan and Report - Audit compares documentation against as built configuration

> Name and nomenclature of company and equipment
>
> List of all documents and revision levels
>
> List of PCA discrepancies and their resolution
>
> Copies of unincorporated changes

Documentation Control System - Written description of acceptable commercial practices implemented within the company

Product Configuration Change Procedures - Formal method of reviewing and evaluating changes as they relate to the Critical Features List

Post Endorsement Physical Configuration Audits (PCA's) - Once a year audit after endorsement by NSA to insure continuing accuracy of documentation and internal monitoring procedures

Parts Control Program - Company established procedures

Facilities/Personnel - Company will support as needed agency PCAs

When the user takes possession of the equipment, engineering changes must be reviewed and approved in writing by the assigned TEMPEST authority for the users organization. When changes to critical items are considered, the decision to re-test is left with the assigned authority.

Making QA decisions can be difficult, since they involve not only a thorough understanding of the current TEMPEST baseline for particular equipment, but also an understanding of how the proposed changes could affect the TEMPEST integrity of the equipment. The table below lists the most common QA concerns faced by TEMPEST authorities involved with routine maintenance of TEMPEST equipment.

***TEMPEST ROUTINE MAINTENANCE***

***There is no set of rules for TEMPEST equipment users to follow on what maintenance should be allowed.***

***There is a requirement that a TEMPEST vulnerability assessment be made before emission protection is necessary.***

***Therefore, Critical Item changes which could adversely affect the TEMPEST profile of the equipment require a new vulnerability assessment.***

***Critical Items which require re-testing when changed are listed on the TEMPEST Critical Features List.***

**Table 1 - Typical QA Concerns**

1. Whether connecting a bond to ground, or mechanically assembling a box, the torque applied will directly affect the impedance of the bolted connection. Another important point is to prevent galvanic corrosion using dissimilar metals.

2. Assembly and repair cleaning instructions, not only for bolts used but for all metal-to-metal contacts and for gaskets.

3. Braided, shielded cables notoriously begin to break where connectors are clamped on the ends. When the small wires break, shielding effectiveness degrades. After connecting and disconnecting cable assemblies for test purposes several times, the wire braids may degrade and should be examined.

4. You must specify how many times a gasket can be compressed before replacement. Also, the old gasket must be totally removed (including residue), the groove cleaned, and a new gasket put in uniformly (evenly) with no pinch.

Routine maintenance is one concern. However, the technological and practical requirements for repair, upgrade, or reconfiguration of equipment to meet ever-changing needs. Often critical items need to be modified. There is no set of rules for equipment users to follow on what should be allowed. There is, however, a requirement that a TEMPEST vulnerability assessment must be made before TEMPEST emission requirements can be imposed. Therefore, Critical Item changes which could adversely affect the TEMPEST profile of the equipment require a new vulnerability assessment.

Examples of critical features the manufactures would impose on TEMPEST equipment are listed in the following table. A change effecting any of the features listed would either require a re-test of the equipment, or a written TEMPEST vulnerability assessment describing how the anticipated degradation would affect the emission control profile of the users area.

**Table 2 - Examples of Critical Features**

- DESIGN FEATURES
  - ADDITION OF SIGNAL CONDITIONING COMPONENTS
  - ADDITIONAL SHIELDING
  - SPECIAL GROUNDING
- SOFTWARE RESTRICTIONS OR REQUIREMENTS
  - INHERENT FEATURES
  - SLOW TURN-ON OR "QUIETER" INTEGRATED CIRCUITS
  - BANDWIDTH LIMITING OF ANALOG CIRCUITS
  - PARALLEL BUSS SIZE
  - SWITCHING RATE OF POWER SUPPLY
- SPECIAL PARTS
  - POWERLINE FILTERS
  - SHIELDED WIRES AND CABLES
  - GASKETS
  - CONNECTORS AND BACKSHELLS
- DESIGN FEATURES OF NON-ADDED PARTS
  - CURRENT LIMITING OF KEYBOARD SENSE LINES
  - USE OF CAPACITIVE TYPE KEYBOARD
  - STROBE SKEW CONTROL FOR PRINT HEAD DRIVE WIRES
- IMPORTANT TOLERANCES
  - GASKET GAP UNDER COMPRESSION
  - GASKET SURFACE FATNESS
  - PLATING THICKNESS
  - TRANSITION TIME CONTROL
  - PRINT-HEAD SHIELDING DIMENSIONS

IMPORTANT PROCESS

- TORQUE WRENCH USAGE
- FLUX AND SOLDER USED FOR BONDING
- PREPARATION OF GASKET MATING SURFACE
- DISSIMILAR METAL SURFACE TREATMENT
- WIRE ROUTING CONSISTENCY

IMPORTANT MATERIAL

- USE OF STEEL OR ALUMINUM
- USE OF PLATING AND TYPE
- CHEMICAL FILM COATINGS FOR METALS
- GASKET TYPE USED
- CABLE SHIELDING - % OPTICAL COVERAGE

AGE EFFECTS

- GASKET EFFECTS
- REPAIR CONSTRAINTS
- SURFACE CLEANING
- CABLE BRAID BREAKDOWN
- OXIDATION/CORROSION

### MIL-HDBK 232A, Red/Black Engineering-Installation Guidelines

MIL-HDBK 232A is used as the baseline guide for most RED/BLACK facilities. Although superseded in a few specific areas by NACSEM 5203, it is cited as the requirements document in MCO P5510.14, Chapter 5. The document covers all aspects of implementation for RED/BLACK installations, fixed site or mobile. The following sections from MIL-HDBK 232A relate to network guidelines.

*Red/Black Engineering-Installation Guidelines*

*MIL-HDBK 232A*

*Used as the baseline guide for most RED/BLACK facilities.*

*Covers all aspects of implementation for RED/BLACK installations, fixed site or mobile.*

### Local Area Networks

"When a LAN is designed or proposed for the purpose of processing classified information, the topology of the LAN must be determined in order to establish the protective measures required. Two topologies exist: point-to-point and multipoint (multipath). Each requires different protection.  Additionally, the transmission media between LAN nodes becomes a significant issue in defining topology."

### Point-to-point Topology

"A point-to-point topology is characterized by dedicated paths between any two nodes.  The paths are not shared.  A point-to-point network may consist of any number of nodes.  Each path will interconnect only two nodes.  A node must have a path to a node with which it wishes to communicate or must be switched through another node.  This topology lends itself to being designed and installed using existing cryptographic devices to secure each path.  Each node is installed using the RED/BLACK concepts defined in this handbook."

### Multipoint Topology

"The multipoint topology is typically implemented with all nodes interfaced to a single transmission medium.  This configuration allows any node to communicate with any other node in the network.  Present security technology does not permit such a network to exist in the RED/BLACK concept.  Such a network can only be all RED."

### RED Equipment Installation

"The goal of any RED equipment installation is to create physical, electrical, and electromagnetic barriers around equipment that processes classified information in order to prevent that information from being exploited by hostile intelligence service activities.  The design begins by establishing a RED Exclusion Area (REA) within the Limited Exclusion Area (LEA).  The space established to contain the RED processing equipment and related support functions with barriers to exclude all other functions.  The ideal situation is to establish a REA adjacent to a Black Exclusion Area (BEA) such that the LEA is contiguous."

### Equipment Separation

"The separation of equipment in the LEA is dependent upon the class of equipment (TEMPEST, COTS, low/high-level signaling, etc.).  The equipment layout keeps dissimilar equipment separated by at least two inches.  Signal and power runs associated with this installation are also separated by two inches.  Should RED and BLACK signals cross at a 90-degree angle, the separation may be reduced to one inch."

"COMSEC equipment establishes a bench mark for equipment separation.  All RED equipment, including patching and distribution frames, are separated from the COMSEC by at least three feet.  All BLACK equipment is also separated from the COMSEC equipment by three feet."

### Baseband LAN

"Baseband LANs use baseband signaling on a single physical transmission medium.  Data rates of 10Mbps are achieved between nodes, with up to 1,000 nodes possible.  Some nodes exist as terminal servers, each supporting multiple terminals.  Such LANs also use multiple levels of protocol or functional layers.  At the present time, baseband LANs present significant challenges and risks in secure applications.  All users have perpetual connection to all other users."

"In order for a baseband to be secure, it must be installed in a power distribution system (PDS),  All users must operate at the same security level.  Physical security measures must be quite stringent since no RED/BLACK barrier exists to protect the network.  Baseband LANs should be kept as small as possible and should not use gateways to other LANs."

### Protected Distribution Systems

"Situations exist which require RED cable distribution to exit one LEA, traverse one or more lower levels of security, and ingress another LEA.  In such cases, additional security measures are required to protect the information being distributed.  Such protection must make penetration into the distribution media so difficult that is discourages the penetrator, or makes discovery and apprehension a certainty.  The amount of protection depends upon the level of classification of the information, the level of security in the area(s) crossed, and the responsiveness of the security force.  The PDS should be exposed to surveillance.  All joints and covers should be welded.  Pull boxes and accesses must be kept to a minimum.  Cables contained within the PDS should have wire supervision which alerts security personnel should a successful penetration occur."

### New Hardware

New hardware is fully configured when purchased and must be approved through the Evaluated Products List (EPL).  Policy for using approved products is described in Section D.5.0 of DoDS 5200.28.  This section deals with equipment that has undergone a formal evaluation process by NSA.  "Computer security features of commercially produced products and Government-developed or derived products shall be evaluated (as requested) for designation as trusted computer products for inclusion on the Evaluated Products List (EPL)."

### Commercial Off-the-Shelf (COTS) Versus Approved Products

The situation often occurs where an approved item needs to be upgraded or repaired, and either COTS or previously evaluated items are available.  Guidelines for selecting equipment are usually vague and require a thorough technical knowledge of the equipment design and the specific application where it is to be used.  Some suggested guidelines for determining which equipment can be substituted are as follows:

(a)  If a previously approved TEMPEST configuration or subsystem component is to be incorporated, it is permissible without a re-test of the entire system.

(b)  If the AIS is upgraded with non-TEMPEST approved equipment, this upgrade could defeat the entire TEMPEST profile of the equipment.  Therefore, as a minimum, the equipment needs a quick profile test plus a new TEMPEST Vulnerability Assessment.