Appendix A
Determination of Robustness Objective

A Cross Domain Solution (CDS) mediates information flows between domains hosted within the CDS or its connected enclaves. The domains differ in their need for confidentiality, integrity, and availability protection. The robustness required of a CDS is proportional to the risk of the unauthorized access by uncleared/untrusted users to data or services with higher confidentiality, integrity and availability needs. A CDS addresses the confidentiality, integrity, and availability needs of the supported domains through robust domain separation and information flow mediation. Robust access and multilevel CDSs must satisfy the availability needs for hosted data and services; robust transfer and multilevel CDSs msut satisfy the availability needs of the data in transit through the CDS.

FIPS Publication 199 expresses this risk as potential impact on organizations and Individuals as the security for an information type. The generalized format for expressing the security category (SC) of an information type is:

$$SC_{\textit{information type}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\}$$

FIPS Publication 199 defines three levels of potential impact on organizations or individuals. The application of these definitions must take place within the context of each organization and the <u>overall national interest</u>. The *potential impact* is:

- **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

  Amplification: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

- **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

  Amplification: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

- **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Amplification: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Executive Order (EO) 13526, Classified National Security Information, provides a classification system for national security information. The EO is supplemented by other guidance that addresses handling caveats and compartmentation. Classification identifies three primary confidentiality levels of potential damage or potential impact.

- ''**Confidential**'' describes information, the unauthorized disclosure of which reasonably could be expected to cause **damage** to the national security.
- ''**Secret**'' describes information, the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security.
- ''**Top Secret**'' describes information, the unauthorized disclosure of which reasonably could be expected to cause **exceptionally grave damage** to the national security.

Handling caveats and compartmentation identify information where unauthorized access can increase the impact from loss of confidentiality.

DoD 8500.2, Information Assurance Implementation, uses the single term Mission Assurance Category (MAC) to determine the combined requirements for availability and integrity.

- **"MAC III"** describes systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities.
- **"MAC II"** describes systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.
- **"MAC I"** describes systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness.

FIPS Pub 199 and DoDD 8500.2 due not adequately distinguish situations of extreme potential impact to integrity and availability where robust CDSs should be employed. For example, it does not distinguish

between the loss of mission effectiveness of an aviation squadron and the loss of control of the nation's nuclear command authority. For the purposes of this appendix, the terms MAC-Extreme, Integrity-Extreme, and Availability-Extreme are used to express these cases.

This appendix provides a risk model for robustness requirements determination. It combines the features of the relevant legacy and contemporary risk models

CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department Of Defense Trusted Computer System Evaluation Criteria in Specific Environments, 25 June 1985

NRL Report 8897, An Approach to Determining Computer Security Requirements for Navy Systems, Carl Landwehr and H.O. Lubbes, 13 May 1985

Risk Decision Authority Implementation Guide, Versions 2.2 and 2.3 draft.