Security Baseline

User Guide

SECURITY BASELINE

USER GUIDE

This user guide describes the basic expectations for completion of the DSS in Transition (DiT) Security Baseline template. The sections that follow mirror those in the template and provide amplification or explanation as appropriate to assist in the Security Baseline completion. After completion, the Security Baseline should be emailed to the assigned DSS Industrial Security Representative for review.

The Security Baseline is designed for unclassified information only. DO NOT enter classified information in this Security Baseline.

GENERAL

The general section is meant to provide an overview of what a Security Baseline is, its intent, and how it plays into the larger risk management effort. This section contains pre-determined text, and does not have to be updated.

SCOPE

The scope section should identify the boundaries of the security baseline: such as any parts of the company or its operations that are excluded from the security baseline. For example, if part of a multiple facility organization (MFO), each specific facility would identify the security baseline scope as all assets under its singular CAGE, not the entire MFO. One security baseline for each CAGE code entity.

ASSET IDENTIFICATION

Describe the process used for asset identification in this section. An idealized version of the asset identification process includes convening key stakeholders across the organization to contribute what is important in the performance and support of national security, categorizing each asset in the context of the Industrial Base Technology List (IBTL), PIEFAOS, etc., and associating specific program and contract data. These results (i.e. the specific characteristics and information captured for each asset) will be identified in Table A-2. Asset Identification Form.

APPENDIX A.

TABLE A-1 ASSET SUMMARY

The Asset Summary table is a consolidated summary of all identified assets. Each asset for which a Table A-2 Asset Identification Form has been generated and included in the security baseline submission, must be added in a corresponding line item within Table A-1, Asset Summary. This table should be expanded as necessary to capture all identified assets.

Asset Name	IBTL Category	PIEFAOS Category

TABLE A-2. ASSET IDENTIFICATION FORM

Below are instructions and elaboration for each individual field in Table A-2, Asset Identification Form. All fields are mandatory unless specifically identified as optional. This table should be copied as many times as required to document each asset separately.

1. Asset Identification
   - 1.1. Asset Identifier. This is a company-assigned unique identifier used in a database, inventory management systems, etc. This is an optional field.
   - 1.2. Asset Name. This is the common name of the asset.
   - 1.3. Asset Description. The description may include relevant location, size, part numbers, special precautions and considerations, and characteristics. What makes this asset special?

2. CATEGORIZATION
   - 2.1. IBTL Categorization. Categorize the asset in the context of the IBTL: www.cdse.edu/documents/cdse/CI-JobAidSeries-IBTL.pdf
   - 2.2. IBTL Sub-Categorization. Sub-categorize the asset in the context of the IBTL: www.cdse.edu/documents/cdse/CI-JobAidSeries-IBTL.pdf
   - 2.3. PIEFAOS Categorization. Categorize the asset in the context of PIEFAOS: http://www.cdse.edu/documents/cdse/Security-in-Depth-Webinar.pdf.
   - 2.4. Asset Use. Identify if this asset for commercial or government use, or both.
   - 2.5. ITAR/EAR. Identify if this asset is export controlled.
   - 2.6. Foreign Involvement. Identify if this asset is associated with any foreign sales, service, relationships or use.
   - 2.7. Critical Program Information (CPI). Specify if this asset has been identified as CPI by the government. www.cdse.edu/multimedia/shorts/cpi/common/cw/.../CDSE_CPI_Student_Guide.pdf

3. PROGRAM DATA

   The following information specific to the program/contract should be identified for each asset.

   - 3.1. Program Name
   - 3.2. Program Classification
   - 3.3. Contract Number
   - 3.4. Customer POC Name
   - 3.5. Customer POC Title
   - 3.6. Customer POC Phone
   - 3.7. Customer POC Email

4. Security Controls & Protection Measures

4.1. Security Controls & Protection Measures. The facility should provide a description of the security measures currently in place to protect each specific asset. This description should be as in-depth as possible, as it is the focus of DSS review and will inform future suggestions for improvements, enhanced mitigations, and/or countermeasures. The security controls and protection measures in place may be rooted in varying requirements; some may be procedural compliance, others may not. Some driving forces may simply be good security practices; others may be rooted in company policy. Every effort should be made to identify the driving force or requirement behind the security control/protection measure.

4.2. Control Source. Include applicable references & frameworks that drive the security controls (i.e. NISPOM, NIST 800-53, contractual requirements, DFAR, ITAR, EAR, Company Policy, Industry Best Practices, Other). It is understood the security controls and protection measures in place may be rooted in varying requirements; some may be procedural compliance, others may not. Some driving forces may simply be good security practices; others may be rooted in company policy. Every effort should be made to identify the driving force or requirement behind the security control/protection measure.

5. Other Asset Information

5.1. Other Information. Detail other relevant information not captured, or expand upon previous information. For example if an identified asset is a supplier, provide the prime contract number, subcontractor number, and CAGE code (if applicable) for the supplier. This is an optional field.