Designation: ~~F1448 – 93a (Reapproved 2006)~~ F1448 – 12

Standard Guide for Selection of Security Technology for Protection Against Counterfeiting, Alteration, Diversion, Duplication, Simulation, and Substitution (CADDSS) of Products or Documents[1]

This standard is issued under the fixed designation F1448; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

This standard has been approved for use by agencies of the Department of Defense.

INTRODUCTION

Any product or document of value has a ~~high~~ risk ~~level~~ of being counterfeited, altered, diverted, duplicated, simulated, or substituted (CADDSS). The greater the value of the object or item, the greater is the likelihood of CADDSS. Counterfeiting of brand names, designer clothes, accessories, jewelry, and intellectual property ~~is presently assessed~~ was assessed in 2006 as a 60-billion-dollar per year problem worldwide. This dollar figure does not include the losses in the financial community, including banknotes, stocks and bonds, etc., the losses of which are unknown and unreported. Just as counterfeiting and alteration of documents are severe problems in the financial sector, the counterfeiting, alteration, diversion, duplication, simulation, and substitution (CADDSS) of products are life threatening when they relate to aeronautical parts, auto parts, pharmaceuticals, life support equipment, and Department of Defense material. The problem cannot be eliminated, but it can be controlled by using anticounterfeiting technology selected to fit the user's requirements. ~~A check list is needed to specify the user's requirements for anticounterfeiting technology to control one or all of the above-mentioned potential fraudulent problems. Whichever technology, or combination of technologies, is used, the frequency of authentication and the education of personnel or the public using the technology are vitally important in controlling counterfeiting, alteration, diversion, duplication simulation, and substitution (CADDSS) of products and documents.~~

The purpose of this document is to provide an overarching guide to protect against CADDSS. Therefore, it is expected that additional standards will be generated that are more specific to a given product, such as clothing, music and videos (and other data-centric products), medicine, currency, official documentation, vehicles, etc. To protect against CADDSS, several steps have to be taken, which include but are not limited to: *(1)* identification of the CADDSS sensitive product, *(2)* documenting the nature, magnitude of likelihood, and magnitude of impact of different CADDSS on the product, *(3)* list the possible anti-CADDSS solutions available to address the documented CADDSS strategies, and *(4)* develop a strength and weakness analysis for each of the applicable anti-CADDSS solutions. Whichever technology, or combination of technologies, is used, the frequency of authentication and the education of personnel or the public using the technology are vitally important in controlling counterfeiting, alteration, diversion, duplication simulation, and substitution (CADDSS) of products and documents.

1. Scope

1.1 This general guide is intended to assist the user ~~in the selection of anticounterfeiting technology as follows:~~ of the guide in selecting anti-CADDSS technologies to protect their product from CADDSS.

[1] This guide is under the jurisdiction of ASTM Committee F12 on Security Systems and Equipment and is the direct responsibility of Subcommittee F12.60 on Controlled Access Security, Search, and Screening Equipment.

Current edition approved ~~Feb. 1, 2006~~Dec. 1, 2012. Published ~~February 2006~~January 2013. Originally approved in 1993. Last previous edition approved in ~~1999~~2006 as F1448 – 93a ~~(1999).~~(2006). DOI: ~~10.1520/F1448-93AR06.~~10.1520/F1448-12.

1.1.1 By determining what the user's requirements are as related to product or document by completing the user's specific CADDSS versus parameters matrix, and

1.1.2 By comparing the user's requirements matrix to a security technology feature matrix prepared by a knowledgeable person using the CADDSS versus parameters matrix.

1.2 This guide does not address or evaluate specific anti-CADDSS technologies, but rather providessuggests a path when utilizing the matrix that assists in Table 1 that allows proper the objective evaluation of features of anti-CADDSS technologies available for use in the application.protection of their product from CADDSS.

1.3 This guide provides a procedure to accomplish the proper selection of a security system. Specific technologies are not addressed, nor isare any technologytechnologies recommended. There are many security systems available in the public marketplace today. Each has limitations and must be carefully measured against the parameters presented in this guide. Once this careful analysis is done, the user will be in a knowledgeable position to select a security system to meet his needs.

2. Referenced Documents

2.1 *ASTM Standards:*[2]

F1156 Terminology Relating to Product Counterfeit Protection Systems (Withdrawn 2001)[3]

2. Terminology

2.1 *DefinitionsDefinitions:*—For definitions of terms used in this guide, refer to Terminology F1156.

2.1.1 *alteration*—the modification of a document or article an object or item that is not the genuine object or time with the intent that it will pass as genuine with minimum risk of detection in circumstances of ordinary use.the genuine object or item.

2.1.2 *counterfeit*—a reproduction of a document, article, or genuine object or item or security feature that is intended to deceive the close scrutiny of thereof so that the reproduction can pass as genuine after detailed inspection by a qualified examiner.

2.1.3 *diversion*—the distribution and sale of legitimate products through unauthorized dealers.a genuine objects or items through unauthorized dealers, often resulting in tax evasion.

2.1.4 *duplication*—the reproduction of a document or part thereof by means of a photoreproductive device.genuine object or item so that reproduction generally looks like the genuine object or item.

2.1.5 *simulation*—the imitation of a document or article, article genuine object or item, or features thereof, including similar security features, in a form that is intended to pass as genuine in circumstances of ordinary use.features.

2.1.6 *substitution*—the act of putting or using one documentobject or item in place of another; within this context, the substituted document or item often is of lesser quality or value.the genuine object or item.

2.2 In all cases, it is assumed the object or item generated by CADDSS is *(1)* of lesser quality and cost than the genuine object or item or *(2)* intended to deceive the party in possession of the CADDSS generated object or item and to do this with a low likelihood of detection or discovery, or both.

4. Summary of Guide

4.1 The six steps in selecting anticounterfeiting technology are as follows:

4.1.1 Define the CADDSS problem,

4.1.2 Determine requirements by using the CADDSS matrix (see Table 1),

4.1.3 Select one or more appropriate matrix technologies by comparison of user's matrix with a technology matrix,

4.1.4 Test by a qualified individual or forensic laboratory for effectiveness,

4.1.5 Implement technology, and

4.1.6 Institute educational program to use technology effectively.

3. Significance and Use

3.1 This guide is the first known attempt to focus on security requirements and compare them to available and known technologies capable of meeting these requirements. This guide provides for the following three steps:describes several steps to select the appropriate anti-CADDSS technology. These steps are described in Section 4.

5.1.1 The user develops a detailed matrix analysis (see Table 1) to identify specific security requirements.

5.1.2 The user obtains a similar matrix that identifies the capabilities of available technologies to satisfy specific security requirements. This matrix can be prepared by the user, by a security consultant, or by a technology vendor. If the user desires, the available technologies matrix can be tested and evaluated by a forensic laboratory.

5.1.3 The user compares these two matrices in order to select one or more technologies that most closely accommodates the user's specific security requirements.

6. Measuring Parameters

6.1 A typical list of measuring parameters employed by the users to detect CADDSS is found in Table 1.

7. Available Technologies

7.1 *Traditional Security Technology:*
7.1.1 Watermarks.
7.1.2 Intaglio printing.
7.1.3 Ultraviolet ink (visible and invisible).
7.1.4 Diphenyl ink.
7.1.5 Fugitive ink.
7.1.6 Infrared ink.
7.1.7 Biorefringent ink.
7.1.8 Metameristic ink.
7.1.9 Hot foil stamping.
7.1.10 Rainbow printing.
7.1.11 Fine line printing (guilloches and lathework).
7.1.12 Photochromic ink.
7.1.13 Planchettes.
7.1.14 Specialty papers.
7.1.15 Thermochromic ink.
7.1.16 Micro lettering.

7.2 *Patented and Proprietary Anticounterfeiting Technology*—One source for determining where available patented and proprietary information may be obtained is the (non-profit) International Anticounterfeiting Coalition, Inc. (IACC).[4] Another source is the *Register of AntiCounterfeiting and Forgery Technologies*.[5]

NOTE 1—When other sources have been identified, inclusion in future revisions will be considered.

8. Forensic Laboratory Evaluation of Security Technologies

8.1 The following are suggested details for evaluation of security technologies by a forensic laboratory:
8.1.1 Photo-mechanical evaluation.
8.1.2 Laboratory simulation.
8.1.3 Mass reproduction analysis.
8.1.4 Testing on a variety of color copiers (including laser types).
8.1.5 Testing on a variety of black and white copiers.
8.1.6 Chemical analysis.
8.1.7 Laser scanner simulation.
8.1.8 Electronic simulation.
8.1.9 Tamper testing.

9. Procedure

9.1 This guide is utilized to define the CADDSS problem as it relates to the user's products or documents.

9.2 By using the matrix (Table 1), the user can specify the requirements needed for CADDSS technology.

9.3 The user requirement matrix is compared to matrices set up for available technologies (5.1.2).

9.4 The user selects and implements a system after evaluation and forensic laboratory testing (see Section 8).

9.5 The final step is to initiate an educational program for proper implementation and authentication procedures to control counterfeiting, alteration, diversion, duplication, simulation, and substitution (CADDSS) of documents or products.

4. Matrix (Fig. 1) Selection Guide for Anti-CADDSS Technology

4.1 The vertical axisIdentify and develop Ya of the matrix identifies the potential problem. The horizontal axis tabulated list of the object(s) or item(s) susceptible X identifies the possible technical requirement to aid in the evaluation of available technologies.to CADDSS.

4.2 Determine the type, likelihood, and magnitude of effect of CADDSS for each of the object(s) or items(s) identified in 4.1. Table A1.1 provides an example documentation of such a determination. The entries in Table A1.1 may contain links to maps, tabulated data, and graphs, or may contain this information directly.

4.3 For each type of CADDSS determined in 4.2, list all possible and appropriate anti-CADDSS strategies and technologies.

4.4 Each parameter is considered by the person responsible for selection of an effective security system, while keeping in mind the requirements in the application.Identify the most desirable candidate anti-CADDSS program by doing the following:

4.4.1 To facilitate selection of an anti-CADDSS program, develop a table similar to that in Table A1.1 except with information contained in the three rightmost columns replaced by a single value (see Table A1.2).

4.4.2 The user then determines an appropriate weighting factor for each of the elements of Table A1.2 listed under the column labeled "%" and places this weight in the column labeled "weight."

4.4.3 Multiply the weighting factor by the table entry, as shown in Table A1.2, and enter in the column labeled "product."

4.4.4 Sum the products found in 5.4.3 and enter in the leftmost column labeled "decision values." These values will be the basis upon which a user will determine if an anti-CADDSS program will be considered.

4.4.5 The user determines the lower limit for a decision value below which an anti-CADDSS program will not be initiated. This lower limit may be based on resources, public acceptance, safety, etc.

NOTE 1—The information generated thus far indicates the importance, to the user, of different CADDSS threats on products. Moreover, the user has defined a threshold of CADDSS threats below which the user will not address, which helps to focus resources on the threats most likely to cause harm, damage, or loss to the user. This assessment is dynamic and can and should be revisited periodically.

4.4.6 Once the above CADDSS threat assessment has been completed, the user must identify the possible anti- CADDSS solutions. To identify these solutions requires an analysis of the application-specific or productspecific anti-CADDSS strategies and technologies. Identification of these solutions is beyond the scope of this standard. It is recommended that separate anti-CADDSS standards development working groups be started for the purpose of generating these application-specific or product-specific anti-CADDSS standards. To assist those standards development working groups, suggestions on how to proceed are now given (it is assumed that the working group is addressing unique applications or products):

4.4.6.1 Identify and tabulate the possible anti-CADDSS solutions for each CADDSS threat determined previously. As an example, Table A1.3 lists arbitrary anti-CADDSS solutions in the leftmost column and, in the adjacent column, the operational, performance, and use parameters of those solutions for the CADDSS threats. As mentioned in the caption of Table A1.3, these anti-CADDSS operational, performance, and use parameters may include, but are not limited to, cost of use, cost of authentication, ease of application/use, ease of authentication, training requirements, experience required to use, experience required to authenticate, evidentiary requirements, evidentiary use, ease of altering, permanence, and safety. The two leftmost columns of Table A1.3 should be generated by individuals knowledgeable of the anti-CADDSS solutions appropriate for a given CADDSS threat.

4.4.6.2 Fill the cells in the table, under "CADDSS Threats," with user-specified ratings that show the importance of the given parameter to the threat. Unless otherwise specified by the user, the value of the rating should be an integer in the range between 0 and 10.

NOTE 2—The information generated by Table A1.3 indicates the importance of different anti-CADDSS solutions to given CADDSS threats for the user. The ratings provide information to the user for selection of an anti- CADDSS solution or solutions. For example, it can provide *(1)* the anti-CADDSS solution that has the highest rating for all CADDSS threats, *(2)* the anti-CADDSS solution rated highest for a given threat, *(3)* the anti-CADDSS parameter of most importance to the user, etc.

4.4.6.3 Compare the CADDSS threats from Table A1.2 to Table A1.3 entries. Those anti-CADDSS solutions that have the highest rating, from Table A1.3, and that simultaneously address the CADDSS threats exceeding the limiting value, from Table A1.2, are likely anti-CADDSS solutions.

4.4.7 Once an anti-CADDSS solution is identified, it should be tested to ensure its effectiveness. Testing should be done by a qualified laboratory to test per the performance, operational, or use parameter deemed important (see Table A1.3).

4.4.8 Upon a successful outcome of the testing of the anti-CADDSS solution, the solution can be implemented.

~~10.3 The analyst places an "X" in the appropriate location under the parameter and across from one of CADDSS.~~

5. Application Suggestions for Anti-CADDSS Technology

5.1 Institute educational program to use anti-CADDSS technology effectively.

5.2 Develop surveillance program to continuously monitor effectiveness of the implemented anti-CADDSS solution.

5.3 Document results and disseminate to appropriate groups and organizations.

5.4 Protect and maintain confidentiality of information to prevent advancement of CADDSS.

6. Keywords

6.1 CADDSS; counterfeit protection; product protection; security; security analysis