Designation: F1448 – 16

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.

INTRODUCTION

Any product or document of value has a risk 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 was assessed to have a total global value of $650 billion in 2008, with 2015 projections exceeding $1 trillion, and employment losses of approximately 2.5 million. 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.

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 of the guide in selecting anti-CADDSS technologies to protect their product from CADDSS.

1.2 This guide does not address or evaluate specific anti-CADDSS technologies, but rather suggests a path that assists in the objective evaluation of features of anti-CADDSS technologies available 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 are any technologies 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. Terminology

2.1 *Definitions:*

[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 Oct. 1, 2016. Published October 2016. Originally approved in 1993. Last previous edition approved in 2012 as F1448 – 12. DOI: 10.1520/F1448-16.

2.1.1 *alteration*—the modification of an object or item that is not the genuine object or time with the intent that it will pass as the genuine object or item.

2.1.2 *counterfeit*—a reproduction of a genuine object or item or security feature 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 a genuine objects or items through unauthorized dealers, often resulting in tax evasion.

2.1.4 *duplication*—the reproduction of a genuine object or item so that reproduction generally looks like the genuine object or item.

2.1.5 *simulation*—the imitation of article genuine object or item, or features thereof, including similar security features.

2.1.6 *substitution*—the act of putting or using one object or item in place of 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.

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 describes several steps to select the appropriate anti-CADDSS technology. These steps are described in Section 4.

4. Selection Guide for Anti-CADDSS Technology

4.1 Identify and develop a tabulated list of the object(s) or item(s) susceptible 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 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 product-specific 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.

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

ANNEX

(Mandatory Information)

A1. EXAMPLE TABLES

A1.1 This annex contains example tables referenced in Section 4.

TABLE A1.1 CADDSS Susceptibility Assessment for {Insert Object or Item Name}

NOTE 1—Each of these metrics should be based on previous experience, observations, or official reports, or a combination thereof. Furthermore, these metrics should include information on the geographic inhomogeneities and periodicity of CADDSS use. Consequently, each table entry could comprise maps and timelines.

CADDSS Type	Likelihood of Use (%)[A]	Extent of Use (%)[B]	Magnitude of Effect (%)[C]
Substitution			
Simulation			
Duplication			
Diversion			
Alteration			
Counterfeit			

[A]This metric represents the likelihood that this particular CADDSS method will be used. The values in this column should sum to 100 %.
[B]This metric represents the percentage of the CADDSS objects or items relative to the total number of the original objects or items. This column does not need to sum to 100 % because all CADDSS threats are likely to be only a fraction of the total number of original objects or items.
[C]The metric should reflect the cost magnitude of the effect of the CADDSS objects or items on the market for the original objects or items. This column will not sum to 100 % and should reflect the financial or other measurable impact.

TABLE A1.2 CADDSS Selection Work Table for {Insert Object or Item Name}

NOTE 1—The column labeled "%" contains a single value, defined by the user, to represent the possible graphic and tabular data presented in each cell of Table A1.1. The weights are user-specified and indicate the amount of importance the user places on each entry of the table. For each column, the values of the weights should range between 0 and 1.0 and sum to 1.0, unless otherwise specified by the user. The column labeled "product" contains the product of the entries in the columns labeled "%" and "weight." The value placed in the rightmost column labeled "Decision Value" is the sum of the values contained in the three columns labeled "product."

CADDSS type	Likelihood of use			Extent of use			Magnitude of effect			Decision Value
	%	weight	product	%	weight	product	%	weight	product	
Substitution										
Simulation										
Duplication										
Diversion										
Alteration										
Counterfeit										

TABLE A1.3 CADDSS Threats and Possible Anti-CADDSS Solutions for {Insert Object or Item Name}

NOTE 1—The label "T/S#" is a place keeper for the different possible anti-CADDSS technology or strategy solutions. The label Pa,b is the performance or use parameter for different anti-CADDSS solutions. The performance and use parameters may include 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, safety, etc. The cells under "CADDSS Threat" should contain the importance of the different anti-CADDSS technology/strategy parameters to the given CADDSS threat. The value in each cell should contain a rating that ranges from 0 to 10. There is no restriction on redundancy of using a given rating.

Anti-CADDSS Solutions		CADDSS Threat					
		Substitution	Simulation	Duplication	Diversion	Alteration	Counterfeit
Technology/Strategy	Operational, performance, or use parameter						
T/S#1	$P_{1,1}$						
	$P_{1,2}$						
	.						
	.						
	.						
	$P_{1,n}$						
T/S#2	$P_{2,1}$						
	$P_{2,2}$						
	.						
	.						
	.						
	$P_{2,n}$						
	.						
	.						
	.						
T/S#M	$P_{M,1}$						
	$P_{M,2}$						
	.						
	.						
	.						
	$P_{M,n}$						