Project	**IEEE 802.20 Working Group on Mobile Broadband Wireless Access** <http://grouper.ieee.org/groups/802/20/>	
Title	**U.S. Department of Defense Wireless Security Requirements for Sensitive but Unclassified information**	
Date Submitted	**2004-1-9**	
Source(s)	William A. Arbaugh waa@waa-assoc.com WAA Associates, LLC. (443)-283-7641 (443)-283-7643 (Fax)	Paul Nguyen Nguyentp@ncr.disa.mil Defense Information Systems Agency Center for Standards Management - Networks Division (703)-681-2309 (703)-681-2971 (Fax)
Re:	A review of basic security properties and the DOD wireless security requirements for sensitive but UNCLASSIFIED information	
Abstract	This contribution provides a brief review of the DOD requirements for the use of wireless products with sensitive but UNCLASSIFIED information	
Purpose	Informational	
Notice	This document has been prepared to assist the IEEE 802.20 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.	
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.20.	
Patent Policy	The contributor is familiar with IEEE patent policy, as outlined in Section 6.3 of the IEEE-SA Standards Board Operations Manual <http://standards.ieee.org/guides/opman/sect6.html#6.3> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/guide.html>.	

U.S. Department of Defense Wireless Security Requirements for Sensitive but Unclassified information

William A. Arbaugh

Paul Nguyen

Overview

- Information Classification Terms
- Introduction to Information Assurance
- Motivation
- DoD Security Policy Pyramid
- Requirements

Common Information Classification Terms

- Protection for these levels can be provided by commercial off the shelf (COTS) equipment if they meet certain standards and is approved:
  - Unclassified
  - Controlled Unclassified Information (CUI)
  - For Official Use Only (FOUO)

Sensitive But Unclassified (SBU)

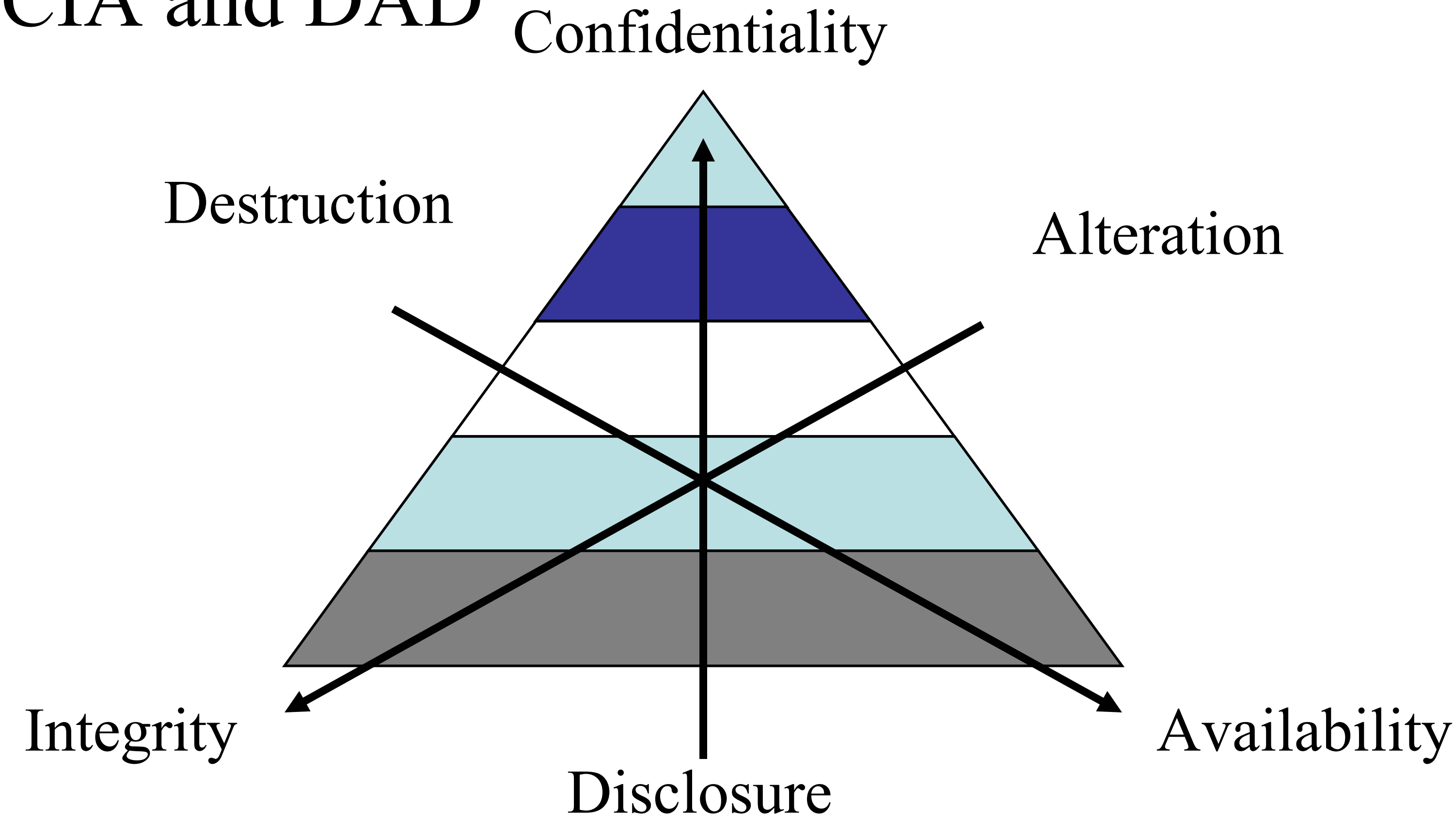
- *A term commonly and inappropriately used within the DOD as a synonym for Sensitive Information, which is the preferred term* (DoDD 8500.1, 2002, p.24).

Information Assurance (IA)

- *Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities* (DoDD 8500.1, 2002, p.20).

Information Assurance (IA)

- CIA and DAD

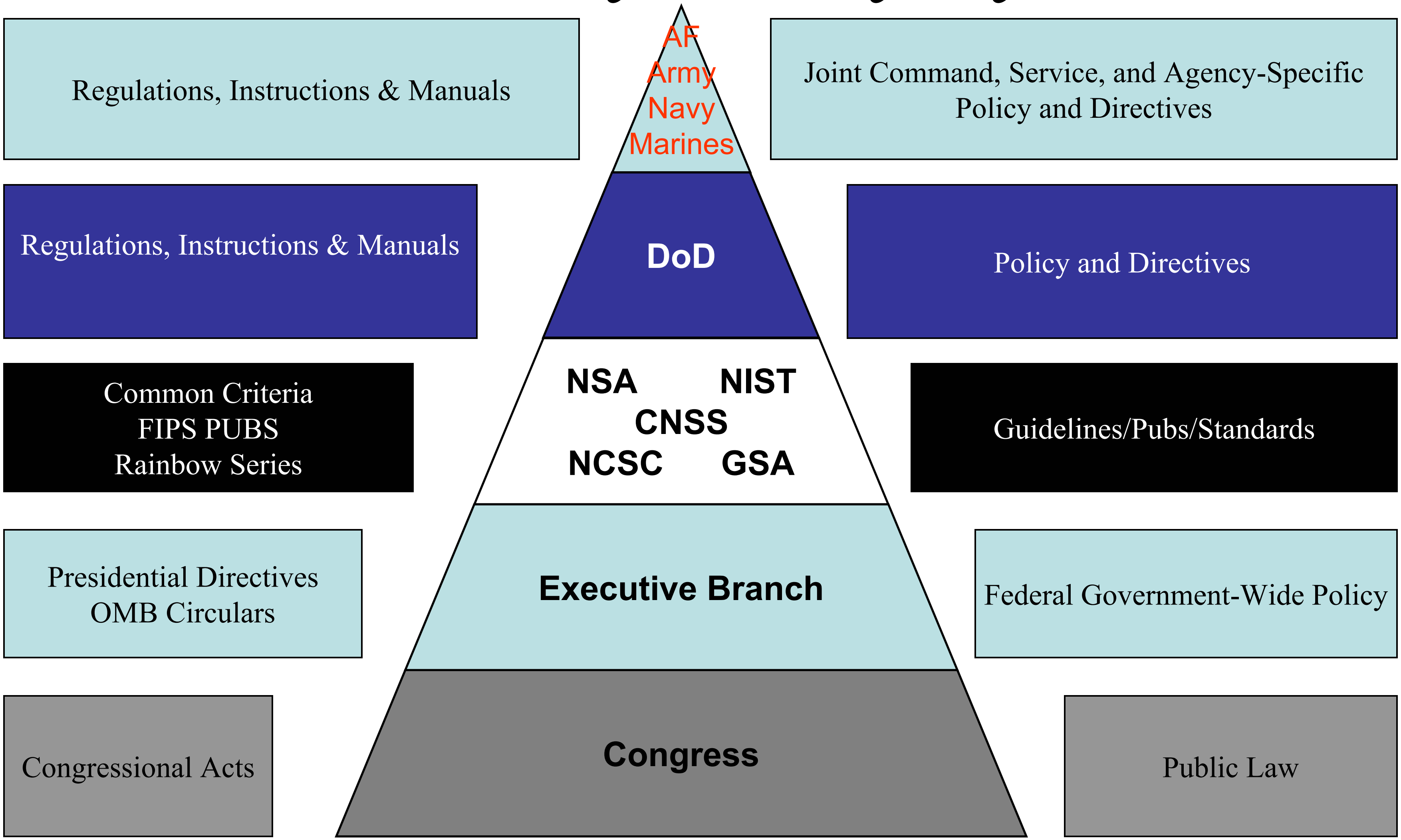


From DISA IA

Motivation

- Why would you want to consider designing your protocol to meet DoD requirements?
  - Requirements mandate the use of “best practice” and the use of well analyzed cryptographic algorithms. In other words, you gain a tremendous increase in assurance at no extra cost!
  - FIPS approved algorithms are patent free.

DoD Security Policy Pyramid



Regulations, Instructions & Manuals

AF
Army
Navy
Marines

Joint Command, Service, and Agency-Specific Policy and Directives

Regulations, Instructions & Manuals

DoD

Policy and Directives

Common Criteria
FIPS PUBS
Rainbow Series

NSA
NIST
CNSS
NCSC
GSA

Guidelines/Pubs/Standards

Presidential Directives
OMB Circulars

Executive Branch

Federal Government-Wide Policy

Congressional Acts

Congress

Public Law

From DISA IA

Summary of Requirements

- Use of FIPS certified cryptographic mechanisms
- Mitigation of Denial of Service attacks
- Use of the DoD Public Key Infrastructure for entity authentication (only if wireless is used for access to the DoD Global Information Grid).

Cryptographic Requirements

- Information Assurance methods that require cryptographic mechanisms, e.g. Confidentiality, Integrity, must use algorithms and modes certified by NIST, e.g. FIPS 140-2.
  - http://csrc.nist.gov/CryptoToolkit/

Confidentiality

- Four algorithms FIPS approved- The only one to consider is AES.
- AES FIPS 197
  - Modes currently under standardization, but it is expected that most all of the DES modes and CCM will be approved.

Non-Repudiation and Integrity

- Digital Signatures
  - DSA, RSA, and ECDSA
- Cryptographic Hashes
  - SHA-1
- Message Authentication Codes
  - HMAC

Availability

- Mitigation of denial of service attacks is vague. The question comes down to the level of effort required by the attacker. If an effective denial of service can be launched with a PDA and a wireless card, then there are problems. The other end of the spectrum is the prevention of RF jamming. This is not cost effective in a COTS product.

Conclusion

- Designing your protocol to meet U.S. Federal requirements is easy; it will increase assurance, and it opens a new market.