DEFENSE CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

Information MUST be classified according to the damage its unauthorized disclosure would cause.

Example: EO 13526 (2009) establishes three classification levels: Confidential (damage), Secret (serious damage), Top Secret (exceptionally grave damage) to national security. SCI (Sensitive Compartmented Information) intelligence sources and methods, accessed only within SCIFs. CUI (Controlled Unclassified Information, 32 CFR 2002) 20 categories including FOUO, law enforcement sensitive, export controlled. Derivative classification creating new documents from classified sources requires training (derivative classifier) and marking per ISOO guidelines. Original Classification Authority (OCA) designated by agency heads.

0.1 2. Clearance & Personnel Security

Access to classified information MUST require appropriate security clearance based on need-to-know.

Example: SF-86 (Questionnaire for National Security Positions) 127-page background investigation form. Adjudication uses 13 guidelines (allegiance, foreign influence/preference, sexual behavior, personal conduct, financial, alcohol, drug involvement, psychological, criminal, IT misuse, handling classified, outside activities, economic). Continuous Evaluation (CE) and Continuous Vetting (CV) replace periodic reinvestigations. Reciprocity clearances accepted across agencies per SEAD-7. Investigation tiers: T1 (low risk), T2 (moderate), T3 (Secret), T4 (high risk), T5 (Top Secret/SCI).

0.2 3. Acquisition

Defense procurement MUST follow DFARS and comply with applicable export control regula-

tions.

Example: DFARS (Defense Federal Acquisition Regulation Supplement, 48 CFR 2) supplements FAR for DoD acquisitions. ITAR (International Traffic in Arms Regulations, 22 CFR 120-130) controls export of defense articles on US Munitions List (USML). EAR (Export Administration Regulations, 15 CFR 730-774) controls dual-use items on Commerce Control List (CCL). Violations: ITAR penalties up to $1.2M per violation or 20 years imprisonment; EAR penalties up to $300K per violation. FMS (Foreign Military Sales) government-to-government. DCS (Direct Commercial Sales) company-to-foreign government with State Department license. Contract types: FFP (firm-fixed-price), CPFF (cost-plus-fixed-fee), CPIF (cost-plus-incentive-fee), T&M (time-and-materials).

0.3 4. Cybersecurity

Defense contractor systems MUST meet CMMC requirements for handling controlled information.

Example: CMMC 2.0 Level 1 (15 practices, self-assessment, FCI), Level 2 (110 practices per NIST SP 800-171, C3PAO assessment, CUI), Level 3 (110+ NIST SP 800-172 enhanced practices, DIBCAC assessment, highest priority CUI). DFARS 252.204-7012 requires adequate security, cyber incident reporting within 72 hours to DC3, and preservation of evidence for 90 days. NIST SP 800-171 Rev. 2 110 security requirements in 14 families for protecting CUI on non-federal systems. NIST SP 800-172 enhanced security requirements for critical programs. POA&M (Plan of Action and Milestones) tracks remediation of gaps.

0.4 5. Supply Chain

Defense supply chain integrity MUST be verified and maintained against counterfeit, compromised, and adversary-controlled components.

Example: SCRM (Supply Chain Risk Management) DoD Instruction 5200.44. Section 889 (NDAA FY2019) prohibits procurement and use of telecommunications equipment from Huawei, ZTE, Hytera, Hikvision, Dahua (Part A: procurement ban, Part B: use ban). Trusted Foundry program DMEA-accredited semiconductor fabrication facilities for mission-critical components. Counterfeit part prevention: SAE AS6171 (test methods), AS6081 (distributors), AS6496 (authorized distribution). GIDEP (Government-Industry Data Exchange Program) shares alerts on nonconforming/counterfeit parts. DLA (Defense Logistics Agency) manages strategic materials and supply chain operations.

0.5 6. Test & Evaluation

Defense systems MUST undergo independent test and evaluation before fielding decisions.

Example: DT&E (Developmental Test and Evaluation) contractor and government testing to verify system meets specifications. OT&E (C5 Test and Evaluation) independent testing under realistic conditions by operational users. DOT&E (Director, C5 Test and Evaluation) statutory office (10 USC 139) that provides independent assessments to Congress for major defense programs. MIL-STDs: MIL-STD-810 (environmental testing), MIL-STD-461 (electromagnetic interference), MIL-STD-882 (system safety). TEMP (Test and Evaluation Master Plan) documents test strategy. DAU (Defense Acquisition University) lifecycle framework: MDD, MSA, MSB, MSC, LRIP, FRP, O&S.

---

1. Constraints

```
MUST:     Cite DFARS clause, MIL-STD, or DoD directive
MUST:     Distinguish between classification levels an
```

```
MUST NOT: Present CUI handling as equivalent to classified information handling
```

DEFENSE | CANON | VERTICALS