Department of Defense
INSTRUCTION

NUMBER O-3600.02
November 28, 2005

USD(I)

SUBJECT: Information Operations (IO) Security Classification Guidance

References: (a) DoD Instruction S-3600.2, "Information Operations Security Classification Guidance (U)," August 6, 1998 (hereby canceled)
(b) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms," as amended
(c) Executive Order 12958, "Classified National Security Information," as amended 25 March 2003
(d) DoD Instruction O-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
(e) through (s), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a) to implement policy, assign responsibilities, and prescribe guidance on the classification methodology for Information Operations (IO) programs and capabilities within the Department of Defense.

1.2. Establishes guidance for proper protection of IO activities.

1.3. Identifies and provides classification guidance on categories of IO activities. While this Instruction identifies the classification or classification range for specific items of classified information, it is not intended to be used as an itemized guide for applying Special Access Program (SAP) protective measures. If required, SAP protective measures shall be in addition to the protections that are cited in this Instruction.

1.4. Addresses the relationship between the protection level for IO activities and the security classification for specific elements of information within these activities. It clarifies information and requirements from a number of sources to identify the appropriate protection architecture for IO activities.

1.5. Constitutes authority and, in the absence of an approved program classification guide that provides specific classification instructions, shall be cited as the basis for derivative classification about, or declassification of, DoD information and material involved in IO.

1.6. Identifies critical program protection issues and guidance to be used as a decision aid by program and security planners to determine if a particular IO program or capability merits the extraordinary security protections found within a SAP.

2. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS

See enclosure 2. Additional terms are defined in Joint Publication 1-02 (reference (b)).

4. POLICY

It is DoD policy that:

4.1. IO programs or tools will consist of those activities where the primary requirement is the logical or physical manipulation, disruption, corruption, or usurpation of human and automated decision making systems. Conventional weapons and other programs, which could be used to achieve an IO effect, but are not specifically designed to affect information or information systems, are excluded from this category.

4.2. The criterion used in the selection of a security classification is the level of damage that would be incurred if a specific piece of information became known. The decision process applied to the selection of a protection level (SAP or non-SAP) is separate and distinct from the decision process involved in the identification and proper security classification (Top Secret, Secret, or Confidential) of the critical information requiring protection. The decision process used in the selection of SAP protection levels focuses on criteria such as the high level of sensitivity of the activity or operation, lead-time advantage, stimulation of adversary's countermeasures, or international sensitivities to a weapon or technology. IO depends on the efficient transfer of sensitive information to be successful. The exchange of information on capabilities and activities between programs is essential to prevent duplication of effort and is critical to ensuring complementary activities achieve the synergy required to be truly effective Warfighting tools. Authorities making Program Protection Decisions and Original Classification Authorities (OCAs) will guard against assigning SAP protection levels and security classifications that are overly restrictive and might prevent or inhibit critical information from reaching those personnel who can best use it, particularly planners and operators in the field.

4.3. Within the Department of Defense, SAPs provide an enhanced level of protection by mandating security measures exceeding those normally required for collateral information, consistent with DoD Instruction O-5205.11 (reference (d)). Activities are designated SAPs to protect unique military capabilities or activities that may have special vulnerabilities or sensitivities. These extraordinary measures are only appropriate for application under circumstances where the vulnerability or sensitivity of the activity makes the additional protective measures essential to the activity's success.

4.4. The security architectures protecting IO systems or tools must be flexible and responsive to provide an appropriate level of protection as these items evolve from concept exploration through development to operations and support. At the same time, the security architecture must allow access for the right personnel to permit the integration of these capabilities into current operations. In order to accomplish these objectives, protection programs will incorporate a "Risk Management" vice "Risk Avoidance" philosophy. Security classification guidance for specific elements of information must be consistent with reference (c).

4.5. Consistency must be achieved in the protection levels and security classifications applied across individual Service and Joint IO efforts. This consistency of protection levels shall be a key element in the successful integration and deconfliction of these activities. For those activities which must, because of their sensitivity, be developed within SAP channels, the program security architecture should allow for the development and release of some program capability information at the collateral level. This information may only address a particular aspect of the total program; however, this collateral "tear line" will be essential to facilitate the integration of the capability into current planning.

5. PROCEDURES

5.1. Classify information based on the potential damage to national security in the areas of foreign affairs, military operations, weapon systems development, and intelligence.

5.2. Overly restrictive protection levels for IO systems and tools can adversely affect the utility and availability of these tools by complicating their inclusion in operational and contingency plans.

5.3. The existence of DoD IO initiatives, the broad concepts and general discussions associated with IO, and the Department of Defense's involvement in IO is unclassified. The fact that conducting IO in the Department of Defense requires the leveraging of functions, processes, and systems, such as the effective design, integration, and interaction among command, control, communications, and intelligence activities, as well as between offensive and defensive capabilities and activities, is also unclassified.

5.4. The fact that the Department of Defense is evaluating the use of, formulating policies for, and developing capabilities associated with offensive IO and IO related systems, to include Computer Network Operations (CNO), Electronic Warfare (EW), Military Deception (MILDEC), Psychological Operations (PSYOP), and Operations Security (OPSEC) is unclassified. Classification of specific capabilities is generally covered under individual component program, system, or operations planning security classification guides. Discrepancies shall be referred to the IO Directorate, Office of the Under Secretary of Defense for Intelligence (OUSD(I)), for resolution.

5.4.1. The minimum classification level for a DoD Computer Network Attack (CNA) capability in which particular technologies, techniques, targets, or concepts are identified shall be SECRET. Higher classification may be warranted based upon the classification guidance for the technologies, techniques, targets, or concepts identified. In these instances, the higher classification shall take precedence.

5.5. Information revealing specific DoD vulnerabilities (other than the known vulnerabilities of widely available commercial products) and the compiled results of vulnerability analyses for all DoD systems shall be classified at a minimum level of SECRET and require appropriate protection levels to control access to the information. Information revealing specific DoD vulnerabilities and the compiled results of vulnerability analyses for unclassified systems is considered sensitive and also requires the application of appropriate levels of control for access to the information. When appropriate, the information will be marked For Official Use Only (FOUO) to ensure a review by the Initial Denial Authority is required before the information so marked is released in response to a request under the Freedom of Information Act (reference (e)). (For specific guidance, see enclosure 3) Publicly available information on general vulnerabilities of commercially available products (e.g., the contents of hacker bulletin boards or vendor websites) should not be classified. However, this information shall be considered for classification when extracted and compiled into a listing of vulnerabilities for which an organization or specific network is deemed susceptible.

5.6. In certain circumstances, the compilation of information identified in this Instruction and other guidance as "unclassified," or derived from open source material, may result in a sensitive or classified product. This may occur when the compilation reveals or details the Department of Defense's specific interest in, or employment of, IO capabilities, techniques, or methodologies; specific DoD vulnerabilities; or, vulnerabilities of the national infrastructure (e.g., systems or equipment, either government or private). The DoD Components shall exercise caution when compiling information consisting of individual terms, items of information, or open source articles concerning IO. When the information is compiled by or for the DoD Components, the information shall be reviewed for marking or classification under the guidance in this Instruction and DoD 5200.1-R (reference (f)). (For specific guidance, see enclosure 3.) Any questions concerning the marking or classification of compiled information shall be referred to the OCA for final determination.

5.7. Release of Information. The fact that this guide shows certain information to be unclassified does not permit automatic public release of information. Proposed public disclosures of unclassified information regarding IO activities must be processed through normal DoD channels prior to the date needed by the individual requesting the release. Procedures governing the release of information apply, but are not limited to, such formats as technical data, articles, speeches, websites, photographs, brochures, advertisements, presentations, displays, and reports.

5.7.1. Release to other U. S. Government Agencies and Contractors. Information marked FOUO, or classified based on the guidance in this Instruction, may be provided to other DoD Components, other U.S. Government Agencies, and U.S. contractors upon determination by the holder of the information that the requester has the proper level of security clearance and requires the information in the performance of official duties, tasks, or functions.

5.7.2. Release to Foreign Governments. Release or disclosure of controlled unclassified information and information classified per this Instruction, must follow disclosure procedures in reference (f) and DoD Directive 5230.11 (reference (g)). Authority is delegated to the Heads of the DoD Criminal Investigative Services to release information marked FOUO per this Instruction, to foreign law enforcement counterparts when the release is required in the timely performance of law enforcement activities. Release of information marked FOUO per this Instruction, by other DoD activities must be coordinated with the OCA and a formal agreement for such disclosure put in place according to DoD Directive 5530.3 (reference (h)).

5.7.3. Requests for Public Release. DoD information requested by the media or members of the public shall be processed according to reference (f), DoD Directive 5230.9 (reference (i)), DoD Instruction 5230.29 (reference (j)), DoD 5400.7-R (reference (k)), and DoD Instruction 5405.3 (reference (l)).

5.8. DoD Information classified under this Instruction shall be processed for declassification according to the provisions in references (c), (e), and ISOO Directive No. 1 (reference (m)). Consult with the head of the organizational Declassification Program for guidance.

6. RESPONSIBILITIES

6.1. The Under Secretary of Defense for Intelligence, as the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for DoD IO, shall:

6.1.1. Provide IO security and program protection guidance and oversee and monitor compliance with this Instruction.

6.1.2. Function as the Office of Primary Responsibility for the maintenance and modification of this Instruction. All inquiries concerning content and interpretation of this Instruction shall be made to the IO Directorate, OUSD(I).

6.2. The Heads of the DoD Components shall ensure compliance with this Instruction when involved with DoD IO and IO related activities.

7. EFFECTIVE DATE

This Instruction is effective immediately.

Stephen A. Cambone
Under Secretary of Defense for Intelligence
NOV 28 2005

Enclosures – 4
- E1. References
- E2. Definitions
- E3. Classification Guide
- E4. Program Protection Specification

E1. ENCLOSURE 1

REFERENCES, continued

(e) Section 552, Title 5 of the United States Code "The Freedom of Information Act"
(f) DoD 5200.1-R, "Information Security Program," January 14, 1997
(g) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(h) DoD Directive 5530.3, "International Agreements," certified current as of November 21, 2003
(i) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," certified current as of November 21, 2003
(j) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
(k) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(l) DoD Instruction 5405.3, "Development of Proposed Public Affairs Guidance (PPAG)," April 5, 1991
(m) ISOO Directive No. 1, "Classified National Security Information, Directive No. 1" 22 September 2003 as amended
(n) DoD 5220.22-M-Sup 1 "Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement," February 1995
(o) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
(p) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(q) DoD Instruction 5215.2 "Computer Security Technical Vulnerability Reporting Program (CSTVRP)" September 2, 1986
(r) DoD Directive O-5205.7, "Special Access Program Policy" January 3, 1997.
(s) Section 119, Title 10 of United States Code

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Computer Network Attack (CNA). Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

E2.2. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity with DoD information systems and computer networks. CND employs IA capabilities to respond to unauthorized activity within DoD information systems and computer networks in response to a CND alert or threat information. Note: CND also employs intelligence, counterintelligence, law enforcement and other military capabilities to defend DoD information and computer networks.

E2.3. Computer Network Exploitation (CNE). Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

E2.4. Computer Network Operations (CNO). Comprise CNA, CND and related CNE enabling operations.

E2.5. Information Operations (IO). The integrated employment of the core capabilities of Electronic Warfare(EW), Computer Network Operations (CNO), Psychological Operations (PSYOP), Military Deception (MILDEC), and Operations Security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own.

E2.6. Information Operations (IO) Program. Those activities that have as a primary requirement the logical or physical manipulation, disruption, corruption, or usurpation of human and automated decision making systems will be included in the category of IO programs or tools. Conventional weapons and other programs, which could be used to achieve an IO effect, but are not specifically designed to affect information or information systems, are excluded from this category.

E2.7. Information Superiority. The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

E2.8. Information System. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, and disseminate information.

E2.9. Military Deception (MILDEC). Those measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.

E2.10. Operations Security (OPSEC). A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) identify those actions that can be observed by adversary intelligence systems; b) determine

indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

E2.11. Psychological Operations (PSYOP). Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objective.

E3. ENCLOSURE 3

CLASSIFICATION GUIDE

The classifications listed in subsections E3.T1.1. through E3.T1.3.8. below are MINIMUM markings or classifications. An OCA may assign a higher classification based on the sensitivity or potential damage to national security. Column 3 provides the marking or classification specification for those items listed in column 2. Columns 3 and 4 provide the classification and the declassification specification according to reference (c). Column 5 provides amplifying guidance on the reason for classification for the element of information. DoD Components shall review a compiled product of individual information items (which, by themselves, may be unclassified,) to determine if it meets the criteria for classification in subsequent specification paragraphs. Unless specifically stated otherwise, the term IO in the following tables applies to all five core capabilities of IO. (See also subsection 5.5.)

Table E3.T1. GENERAL

ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.1.1.	The existence of DoD IO activities and the broad concepts associated with IO and the Department of Defense's involvement across the conflict spectrum and the range of military operations.	UNCLAS	N/A	N/A
E3.T1.1.2.	The fact that the Department of Defense views IO as critical to success in modern warfare and intends pursuing it as a high priority and in a concerted, integrated fashion.	UNCLAS	N/A	N/A
E3.T1.1.3.	General budget information on DoD IO activities.	UNCLAS	N/A	N/A
E3.T1.1.4.	Specific budget information on DoD IO activities (e.g., amounts by particular program).	UNCLAS[1,2,4,5]	N/A	Use handling instructions of FOUO.

Table E3.T1. GENERAL

ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.1.5.	Release of IO information to foreign individuals or organizations.	See Remarks	NA[5]	The release of information shall follow the appropriate foreign disclosure guidance.
E3.T1.1.6.	General discussions of the need to research and develop new methods for conducting IO and intelligence activities in support of IO.	UNCLAS	N/A	N/A
E3.T1.1.7.	The fact that the Department of Defense is pursuing research and technology development in IO.	UNCLAS	N/A	N/A
E3.T1.1.8.	Identification of general technologies as having applicability to IO activities.	UNCLAS	N/A	N/A
E3.T1.1.9.	Identification of general technologies as having applicability to, and being pursued for, improving and/or enabling capabilities for DoD IO.	UNCLAS[1]	N/A	N/A
E3.T1.1.10.	Information which reveals or describes general DoD IO capabilities.	UNCLAS[1,2,3]	N/A	Reference (c) Para 1.4(g) Specific U.S. System IO capabilities are protected under each system security classification guide. Refer to program or operation classification guide for specific information.
E3.T1.1.11.	Information which reveals IO vulnerabilities of DoD systems.	SECRET[1]	See Note[2]	Reference (c), Para 1.4(g) NOTE: This does not include publicly available information on the general vulnerabilities inherent in commercially available products used by the Department of Defense.
E3.T1.1.12	The concept of intelligence support to IO.	UNCLAS[5]	N/A	N/A

Table E3.T1. GENERAL

ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.1.13.	The general concept of intelligence collection and analysis to support DoD IO activities.	UNCLAS[5]	N/A	N/A
E3.T1.1.14.	Specific information about the evaluation, development, acquisition, testing, and fielding of U.S. IO capabilities and techniques.	UNCLAS[1]	N/A	N/A
E3.T1.1.15.	The fact that the Department of Defense views IO as critical to-success in modern warfare and intends pursuing it as a priority mission.	UNCLAS	N/A	N/A
E3.T1.1.16.	Identification of specific technology areas as having applicability to stated DoD IO mission needs.	UNCLAS[1]	N/A	N/A
E3.T1.1.17.	The specific technology being pursued by the Department of Defense in response to a stated IO mission need.	SECRET[1]	See Note[2]	Reference (c), Para 1.4(a).
E3.T1.1.18.	The fact that Intelligence Components of the Department of Defense are involved in the exploitation of automated systems for intelligence and targeting purposes.	UNCLAS	N/A	N/A
E3.T1.1.19.	Details of or specific plans for the Department of Defense's exploitation of automated information systems for intelligence and targeting purposes.	SECRET[1,3]	See Note[2]	Reference (c), Para 1.4(a, c, d). Contact the Proponent or Service Special Access Program Coordination Office (SAPCO) for potential additional protective measures prior to assigning classification.
E3.T1.1.20.	The fact of DoD exploitation of the automated information systems of specific targets (countries or other entities) for intelligence and targeting purposes.	SECRET[1,3]	See Note[2]	Reference (c), Para 1.4(a, c, d). Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.

Table E3.T1. GENERAL				
ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.1.21.	The fact of DoD development of dual-purpose systems (e.g., having application to intelligence exploitation and potentially affecting adversary information and information systems).	UNCLAS[1,8]	N/A	Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification
E3.T1.1.22.	The fact that the Department of Defense is acquiring, developing, testing, and fielding capabilities and techniques for IO purposes.	UNCLAS	N/A	N/A

Table E3.T1. CAPABILITIES				
ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.2.1.	The fact that the Department of Defense is developing IO systems for the purpose of evaluating DoD defensive capabilities.	UNCLAS	N/A	N/A
E3.T1.2.2.	Specific, DoD-unique, CNA capabilities used in evaluation of capabilities.	SECRET[1]	See Note[2]	Reference (c), Para 1.4(g). See Section 3.3.2 and 3.3.3 for protection of vulnerabilities revealed.
E3.T1.2.3.	Broad concept of IO, such as the need to affect, using various means, adversary information, information systems, or target audiences.	UNCLAS	N/A	N/A

Table E3.T1. CAPABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.2.4.	The broad concepts of nodal targeting as a methodology and its significant importance as a tool for IO.	UNCLAS[1,4,5]	N/A	Use handling instructions of FOUO.
E3.T1.2.5.	General discussions of nodal targeting results without specific information as to how the targets are derived.	UNCLAS[1,4,5]	N/A	Use handling instructions of FOUO.
E3.T1.2.6.	General discussion of DoD IO and types of targets, techniques, and capabilities to exploit, deny, or manipulate adversary information, information systems, or target audiences, and the targeted vulnerabilities.	UNCLAS[1,8]	N/A	N/A
E3.T1.2.7.	Identification of specific technologies being pursued solely for CNA.	SECRET[1,8]	See Note[2]	Reference (c), Para 1.4(e). SAP protection may be warranted if the intent of the United States to employ capabilities, fragility of the technique, and/or sensitivity of the target/system to be exploited, could reveal U.S. plans, or cause implementation of countermeasures by adversaries. Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.
E3.T1.2.8.	Identification of novel or unique technologies/techniques, or the novel or unique application of specific technologies and techniques for the purpose of IO.	SECRET[1,8]	See Note[2]	Reference (c), Para1.4(e).

Table E3.T1. CAPABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.2.9.	The specific intent, details of, or specific plans of the Department of Defense to employ an IO technique against a specific target or target audience (countries or adversaries).	SECRET[1,8]	See Note[2]	Reference (c), Para 1.4(a, c, d, g)
E3.T1.2.10.	Specific methods of, or technologies for, intelligence collection and analysis used to identify capabilities for IO and/or vulnerabilities to IO of adversary targets, information, information systems, or target audiences.	SECRET[1,8]	See Note[2]	Reference (c), Para 1.4(c).
E3.T1.2.11.	The fact that the Department of Defense is evaluating capabilities for offensive IO purposes.	UNCLAS	N/A	N/A
E3.T1.2.12.	Specific information about the acquisition, development, testing, and fielding of DoD offensive IO capabilities and techniques, if that information is likely to reveal U.S. plans, cause implementation of countermeasures by adversaries, or adversely impact economic institutions.	SECRET - [1,2,8]	See Note[2]	Reference (c), Para 1.4(a, g). SAP protection may be warranted if the intent of the United States to employ capabilities, fragility of the technique, and/or sensitivity of the target/system to be exploited, could reveal U.S. plans, or cause implementation of countermeasures by adversaries. Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.

Table E3.T1. CAPABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.2.13.	Identity of specific DoD entities and DoD contractors participating in the development, testing, fielding, or execution of offensive IO systems, tools, or weapons.	UNCLAS [1,2,3]	N/A	These activities entail significant OPSEC considerations. Organizations that engage in activities that entail significant OPSEC consideration must consider the threat to and vulnerability of the operation. Refer to program or operation classification guide for specific information.
E3.T1.2.14.	The fact that the Department of Defense has requirements for the use of IO in support of military operations.	UNCLAS	N/A	N/A
E3.T1.2.15.	Specific DoD IO requirements.	SECRET[1]	See Note[2]	Reference (c), Para 1.4(a).
E3.T1.2.16.	General information on U.S. capability to conduct electronic attack operations.	UNCLAS[1]	N/A	N/A
E3.T1.2.17.	Information that reveals details of a DoD CNA capability against a specific country or adversary.	SECRET[1,2,8]	See Note[2]	Reference (c), Para 1.4 (a, d, e). Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.

Table E3.T1. CAPABILITIES

ITEM #	ELEMENT OR CATEGORY OF INFORMATION	MINIMUM CLASS	DECLASS INSTRUCT	REMARKS OR REASON FOR CLASSIFICATION
E3.T1.2.18.	Information that reveals details of a DoD PSYOP capability against a specific country, target audience, or adversary.	SECRET[1],[8]	See Note[2]	Reference (c), Para 1.4 (a, d, e). Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.
E3.T1.2.19.	Information that reveals details of a DoD MILDEC capability against a specific country or adversary, or reveals methods, plans, operations, and indicators of MILDEC operations.	SECRET[1],[8]	See Note[2]	Reference (c), Para 1.4 (a, d, e). Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.
E3.T1.2.20.	Information that reveals details of a DoD OPSEC capability against a specific country or adversary.	SECRET[1],[8]	See Note[2]	Reference (c), Para 1.4 (a, d, e). Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification.
E3.T1.2.21.	Information that reveals U.S. capability to conduct CNA against a specific type of system or technology.	SECRET	See Note[2]	Reference (c), Para 1.4 (a, g).
E3.T1.2.22.	Information that reveals details of U.S. capability to conduct CNA against a specific type of system or technology in a specific country or adversary.	TOP SECRET-SCI[1] -	See Note[2]	Reference (c), Para 1.4 (a, c, d, e).
E3.T1.2.23.	Information that reveals state-of-the-art CNA or access technologies, techniques, or tactics that permit access to closed or proprietary networks or protocols.	TOP SECRET-SCI[1] -	See Note[2]	Reference (c), Para 1.4 (a, c, d, e).
E3.T1.2.24.	Information that reveals the exploitation of fragile vulnerabilities requiring sensitive or specialized intelligence data to execute.	TOP SECRET SCI	See Note[2]	Reference (c), Para 1.4 (a, c).

Table E3.T1. CAPABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.2.25.	Information that may compromise the activities or programs of another Service or Agency.	SECRET[1,2,8]	See Note[2]	Reference (c), Para 1.4 (a, g).

Table E3.T1. VULNERABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.3.1.	General concepts of IO and the need to defend, through various means, one's own information, information systems, processes, and networks.	UNCLAS	N/A	N/A
E3.T1.3.2.	Information on vulnerabilities for commercial off-the-shelf (COTS)systems or components (hardware, firmware, or software) for which the vulnerability information is available within the public domain and there is no value-added analysis by a DoD component.	UNCLAS	N/A	N/A
E3.T1.3.3.	Information on vulnerabilities for COTS systems or components (hardware, firmware, or software) for which the vulnerability information is not available within the public domain or for which there is value-added analysis by a DoD component.	UNCLAS[1,3,4,5,6]	N/A[1,3]	Use handling instructions of FOUO.

Table E3.T1. VULNERABILITIES				
ITEM #	**ELEMENT OR CATEGORY OF INFORMATION**	**MINIMUM CLASS**	**DECLASS INSTRUCT**	**REMARKS OR REASON FOR CLASSIFICATION**
E3.T1.3.4.	Information revealing specific details on vulnerabilities of classified information systems or networks, or IO vulnerabilities of dependent weapon systems used by the DoD Components (e.g., system, location, affected organization or organizations, and methods of attack), and associated plans and systems required to mitigate or eliminate vulnerabilities (e.g., corrective action and status of whether corrective action has been implemented).	SECRET[1,3,4,5,6]	See Note[2]	Reference (c), Para 1.4(e, g).
E3.T1.3.5.	Information on attempted intrusions into unclassified information systems or networks used by the DoD components, for the purpose of securing the networks.	UNCLAS[1,3,4,5,6]	N/A[1,3]	Use handling instructions of FOUO. Note: For information on vulnerabilities which includes the source and impact of an intrusion see E3.T1.3.6.
E3.T1.3.6.	Information on results of allied or coalition network vulnerability analyses performed by or for a DoD Component.	SECRET[1,5,8]	See Note[2]	Reference (c), Para 1.4(b, c, g).
E3.T1.3.7.	General concepts of Computer Network Defense and EW, and the need to defend through various means one's own use of systems processes and networks.	UNCLAS	N/A	N/A
E3.T1.3.8.	Information on vulnerabilities of unclassified information systems or networks used by the DoD Components, which include analysis or assessment of the impact of an attack or attempt to exploit such vulnerabilities; or of the source of an attack or attempt (e.g., organized, state-sponsored, etc).	SECRET[1,3,4,5,6]	See Note[2]	Reference (c), Para 1.4 (b, c, e, g).

[1] Higher classifications and special handling caveats may be required and shall be applied if warranted by program, system, or operations planning classification guidance. Consult appropriate classification guide. Contact the Proponent or Service SAPCO for potential additional protective measures prior to assigning classification. Provisions of DoD 5220.22-M (reference (n)) may apply.
[2] Classification duration is dependent on program, system, or operations planning classification guide. Duration of classification is limited to 25 years unless specifically exempted.
[3] Reports or information will be marked FOUO with protective measures and distribution limitations applied per reference (f) and DoD Directive 8500.1 (reference (o)), and DoD Instruction 8500.2 (reference (p)).
[4] Added consideration must be given to the potential impact of the vulnerability, capability, target, or technique discussed and, at the discretion of the commander, the information classified appropriately through use of program specific classification guidance or tentative classification pending final determination by the OCA.
[5] When sensitive intelligence sources or methods are involved, the information will be classified accordingly.
[6] The DoD Components shall submit reports on vulnerabilities to the Computer Security Technical Vulnerability Reporting Program and CSEC per DoD Instruction 5215.2 (reference (q)).
[7] See subsection 5.6.2. for release to allies, coalition partners, and other foreign governments.
[8] Higher classification, if warranted by the potential impact of the capability, technique, or target. Consult appropriate classification guides and SAPCO for potential additional protective measures prior to assigning classification.

E4. ENCLOSURE 4

PROGRAM PROTECTION SPECIFICATION

This matrix identifies critical program protection issues and shall be used as a decision aid by program and security planners to determine if a particular IO program or activity merits the extraordinary security protections found within a SAP. This matrix is not all inclusive; program and security planners may identify other factors that merit the application of SAP protection. Use in conjunction with the DoD SAP approval process defined in DoD Directive O-5205.7 (reference (r)). IO programs or activities, which have critical program information that falls within one of the areas shown below, may warrant the establishment of a SAP. This decision is generally based upon the unique, technical, or operational sensitivity of the program or activity under consideration. Within the IO arena, the technology "life cycle" is compressed to a degree not normally found in other mission areas. As a result, a program's protection level requires close monitoring to ensure it is appropriate to the capabilities and information the program contains. As the need to protect a capability or technology changes or evolves, program sponsors must ensure that the requirements for program transition or termination contained in reference (f) are followed.

TABLE E4.T1. POLICY SENSITIVITIES

TOPIC	DESCRIPTION
E4.T1.1. TREATY ISSUES	Knowledge of the program or activity.
E4.T1.2. SENSITIVE ACCESS SOURCES AND METHODS	Special access protection required to protect sources and methods.
E4.T1.3. SPECIFIC ACCESS CAPABILITIES OR TECHNIQUES	Purpose of the program cannot be known without compromising its activities and generating adversary countermeasures.
E4.T1.4. INTRUSIVE INTELLIGENCE REQUIREMENTS	Obtaining the intelligence needed for the system to be effective could expose the program or activity, if not protected within a SAP.
E4.T1.5. WEAPON EFFECTS (AMBIGUOUS OR UNAMBIGUOUS)	Existence and purposes of program or activity cannot be known without compromising its objectives.
E4.T1.6. EQUITIES OF ALLIES	Program or activity could impact national foreign policy or diplomatic posture.
E4.T1.7. SENSITIVITIES OF INTERNATIONAL COMMUNITY	Program or activity could impact national foreign policy or diplomatic posture.

TABLE E4.T2. TECHNICAL SENSITIVITIES	
TOPIC	DESCRIPTION
E4.T2.1. SENSITIVE ACCESS SOURCES AND METHODS	Special access protection required to protect sources and methods.
E4.T2.2. SPECIFIC ACCESS CAPABILITIES OR TECHNIQUES	Purpose of the program cannot be known without compromising its activities and generating adversary countermeasures.
E4.T2.3. TECHNICAL SENSITIVITY – LEAD TIME ADVANTAGE	Activity or program represents a battlefield force multiplier, which provides significant advantages in the areas of offense, defense, technology, and intelligence.
E4.T2.4. COST OF COUNTERMEASURES	Cost of countermeasures for the program or activity is inexpensive and would negate U.S. capability.
E4.T2.5. WEAPON EFFECTS (AMBIGUOUS OR UNAMBIGUOUS)	Existence and purposes of program or activity cannot be known without compromising its objectives.

TABLE E4.T3. OPERATIONAL SENSITIVITIES	
TOPIC	DESCRIPTION
E4.T3.1. SPECIFIC ACCESS CAPABILITIES OR TECHNIQUES	Purpose of the program cannot be known without compromising its activities and generating adversary countermeasures.
E4.T3.2. TECHNICAL SENSITIVITY – LEAD TIME ADVANTAGE	Activity or program represents a battlefield force multiplier, which provides significant advantages in the areas of offense, defense, technology, and intelligence.
E4.T3.3. INTRUSIVE INTELLIGENCE REQUIREMENTS	Obtaining the intelligence needed for the system to be effective could expose the program or activity if not protected within a SAP.
E4.T3.4. WEAPON EFFECTS (AMBIGUOUS OR UNAMBIGUOUS)	Existence and purposes of program or activity cannot be known without compromising its objectives.
E4.T3.5. SENSITIVITIES OF INTERNATIONAL COMMUNITY	Program or activity could impact national foreign policy or diplomatic posture.

*Note: Additional restrictions/protective measures, as specified in Section 119, Title 10 of United States Code (reference (s)), may be appropriate