# *Critical Program Information (CPI) Test Vector*

**NDIA SE Symposium #16290**

Geoff "Ninja" Donatelli
Engineering Fellow
Sys Security Engineering Tech Director
Raytheon Missile Systems
520.794.7206
Ninja.Donatelli@raytheon.com

# Critical Program Information (CPI): Today

- Challenges in applying current definition:
    - **Ambiguity** leading to lack of **Repeatability**
        - Ambiguity: many programs will not declare item as CPI
        - Different teams come to different conclusions
        - Evidence: CPI identified by contractors regularly exceeds the # of CPI identified by the Army Research Technology Protection Center (ARTPC)*
        - Consistency is important to industry in competitive bids
        - Failure to detect CPI
    - **False Alarms** – declaring CPI when item is not sensitive
- Current definition under revision by DoD
- How can the government evaluate multiple CPI definitions?

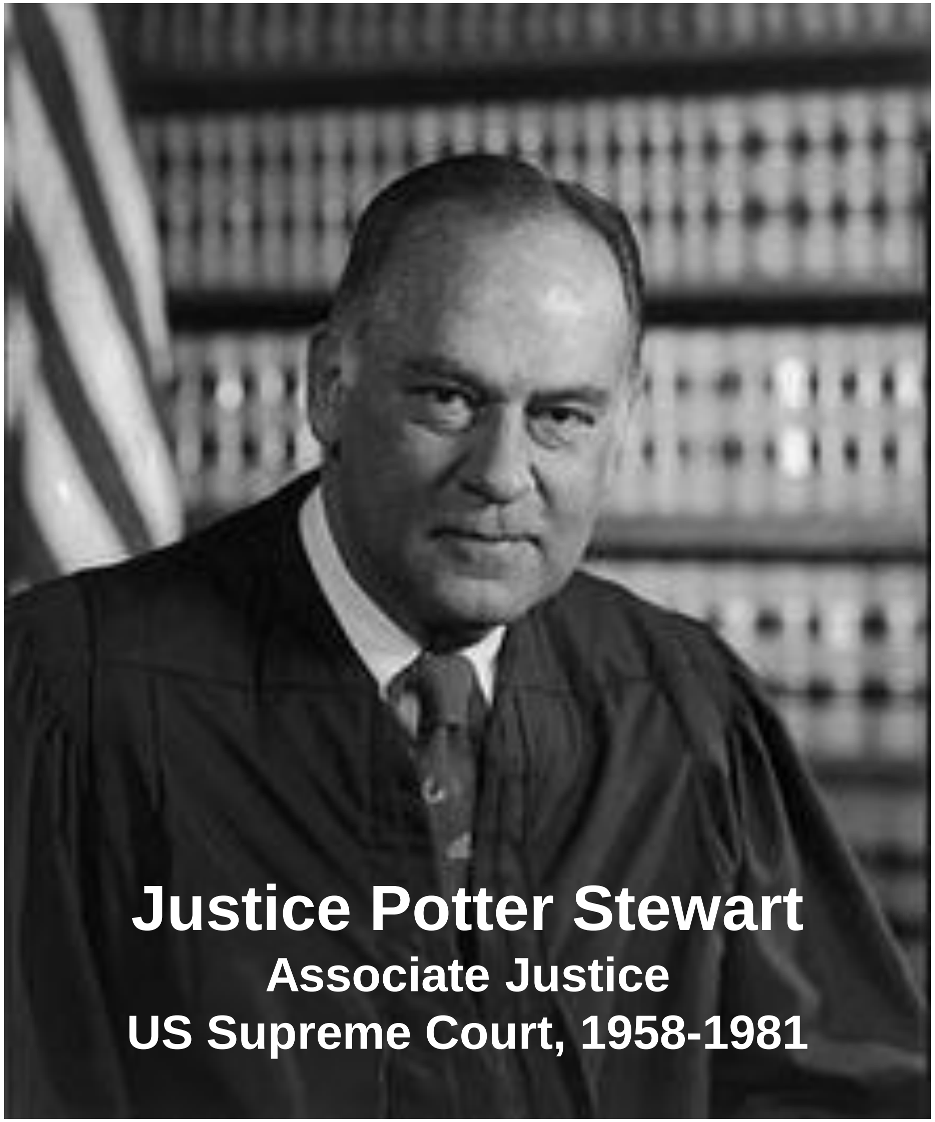
**** Source: USA AT V&V Office***

# CPI Test Vector Methodology

- “Test vector” can evaluate whether a proposed definition will:
  - Minimize ambiguity, and allow independent teams evaluating the *same system* to reliably identify the same CPI
  - ***Not*** identify CPI that does not deserve protection (low false alarms)
- 29 candidate CPI identified to test the CPI definition by *exploring the boundaries*
- Surveyed government and industry AT leaders at the Feb 2013 “AT Summit” to establish “truth”
- Compared the 29 candidates to the three CPI definitions: Declared CPI? Not declared CPI?
  - Compared with survey “truth”

# Critical Program Information (CPI) Definition

**"…I know it when I see it…"**



**Justice Potter Stewart**
**Associate Justice**
**US Supreme Court, 1958-1981**

# CPI Definition

- Current CPI definition, DoD 5200.39, 7/16/2008
  - *"Elements or components of an RDA program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability."*
- CPI definition used by DoD and industry to identify sensitive information, and is crucial to the DoD Anti-Tamper process
  - Anti-Tamper (AT) is often the domain that identifies CPI
- Additional guidance available in the Defense Acquisition Guide (DAG)

# *How Objective is CPI Identification?*
# *"CPI Test Vector" Survey at AT Summit**

- Surveyed 26 government and industry experts to establish "Truth," Feb 2013, "AT Summit"
  - Provided 29 CPI technology candidates
  - Identified CPI by "gut feel," rather than using a CPI definition
  - Included leaders of AT for each service and primes
- Each of the 29 candidate CPI was judged "yes" (positive for CPI) if weighted average >50%; "no" if <50%
  - Government weighted 80%
  - Contractors with CPI ID experience weighted 20%

* *AT Summit, Feb 2013*

* * *% of AT Summit vote. If multiple CPI candidates, this is the average.*

# “CPI Test Vector” Survey Results

- Consensus CPI (**):
  - Technologies providing warfighting advantage (100%)
  - Technologies that could lead to the development of countermeasures (100%)
  - Technologies recognized as CPI by other programs (98%)
  - Unique manufacturing process (90%)
  - 5230.28 technologies, non-COTS (87%)
  - Anti-Tamper know-how (83%)
  - Export license proviso preventing modification (80%)
  - COMSEC keys that could allow eventual decryption of classified information long after encrypted data is collected (80%)
  - Classified that is US only (69%)
  - Integrated system where there is no CPI at the component / element level, but as an integrated whole system, is unique and provides a warfighting advantage (66%)

*  *AT Summit, Feb 2013*

* *  *% of AT Summit vote.  If multiple CPI candidates, this is the average.*

# "CPI Test Vector" Survey Results

- **Consensus of candidates NOT CPI:**
  - Classified parameters which may be shared with export customers, such as system performance (34%)
  - Previously identified as CPI, but reduced in capability for export. No longer provides technology advantage or would degrade mission effectiveness if compromised. (29%)
  - Technologies offering significant reduction in cost (but not affecting performance) (24%)
  - LO/CLO technologies NOT breaking 5230 (24%)
  - Unclassified performance (23%)
  - MCTL item, not otherwise CPI (18%)
  - ITAR, not otherwise CPI (insufficient condition) (16%)
  - Technology not otherwise CPI, but is being exported (8%)
  - COTS (0%)

# Analysis of AT Summit Survey ("Truth")

- Weak or no consensus
  - Operational data, such as waypoints (48%) or target location data (55%) (average: 52%)
    - » Post-survey discussion seemed to indicate there could be value to an exploiter to know whether airspace violations may have occurred, or that might prove embarrassing to the US)
  - GPS keying material (55%)
    - » Post-survey discussion seemed to indicate there would be no value to an exploiter, as this is perishable

# CPI Test Vector: Evaluation

- Evaluated three CPI definitions plus truth
  - 5200.39 CPI definition
  - 5200.39 plus Defense Acquisition Guidebook (DAG)
  - Proposed National Defense Institute Association (NDIA) definition
  - Compared to “truth” from Survey of AT Summit
- Where ambiguities were found, default answer is “no CPI” for that item

# CPI Test Vector:
## Comparison of Definitions with "Truth" Summary

| | | | CPI Def'n Alone | | CPI + DAG | | NDIA Def'n | |
|---|---|---|---|---|---|---|---|---|
| | Truth:Defn' | | Count | Percent | Count | Percent | Count | Percent |
| Disagreements with "truth" | Y:N+N:Y | | 11 | 38% | 12 | 41% | 5 | 17% |
| Correctly identified CPI | Y:Y | | 8 | 50% | 10 | 63% | 14 | 88% |
| Missed CPI | Y:N | | 8 | 50% | 6 | 38% | 2 | 13% |
| False Alarms | N:Y | | 3 | 23% | 6 | 46% | 3 | 23% |
| Correctly passed over non-CPI | N:N | | 10 | 77% | 7 | 54% | 10 | 77% |

**REFERENCES:**

[1] DoD 5200.39, 7/16/08, including Change 1, 12/28/10

[2] Defense Acquisition Guidebook (DAG), 10/9/12

[3]Proposed CPI Definition, NDIA, 2012

- **Definition of CPI alone: Correctly detects 50% of CPI that are "true" CPI**
  **Missed 50% of "true" CPI**
  **Identified 23% of "false" CPI as CPI**
  **Correctly passed over 77% of non-CPI**
- **CPI plus DAG definition: Correctly detects 63% of CPI that are "true" CPI**
  **Missed 38% of "true" CPI**
  **Identified 46% of "false" CPI as CPI**
  **Correctly passed over 54% of non-CPI**
- **Proposed NDIA Definition: Correctly detects 88% of CPI that are "true" CPI**
  **Missed 13% of "true" CPI**
  **Identified 23% of "false" CPI as CPI**
  **Correctly passed over 77% of non-CPI**

# CPI Test Vector: Conclusion

- Testing CPI definitions for accuracy and consistency is essential
- Even a panel of experts at the AT Summit can give a wide variance of opinions on what constitutes CPI
- Definition requires additional detailed guidance to properly implement
    - Fielding new CPI definition without additional guidance, or leaving current guidance in place (DAG), can conflict and have adverse effects
    - Recommend fielding new definition simultaneous with additional guidance
- Additions to candidate CPI, or modifications to the methodology are welcome

# QUESTIONS?

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| Simplistically, Critical Program Information (CPI) should be thought of as the technological "crown jewels" of the program. The United States gains military advantages from maintaining technology leads in key areas, so we must protect them from compromise in the development environment and on fielded systems. | - Crown jewels<br>- US technology lead |
| Critical Program Information (CPI) may include classified military information which is considered a national security asset that will be protected and shared with foreign governments only when there is a clearly defined benefit to the United States (see DoD Instruction 5200.39). It may also include Controlled Unclassified Information (CUI), which is official unclassified information that has been determined by designated officials to be exempt from public disclosure, and to which access or distribution limitations have been applied in accordance with national laws and regulations such as the International Traffic in Arms Regulations for U.S. Munitions List items and the Export Administration Regulations for commerce controlled dual-use items. In some cases (and this is dependent on the program manager's determination) a commercial-off-the shelf (COTS) technology can be designated Critical Program Information (CPI) if the commercial-off-the shelf (COTS) element is determined to fulfill a critical function within the system and the risk of manipulation needs mitigation. | - May include classified information<br>- May include Controlled Unclass Info, such as ITAR, exempt from public release<br>- May include COTS if element is a critical function and risk of manipulation needs mitigation |

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| Critical Program Information (CPI) requires protection to prevent unauthorized or inadvertent disclosure, destruction, transfer, alteration, reverse engineering, or loss (often referred to as "compromise"). | |
| Critical Program Information (CPI) identified during research and development or Science and Technology should be safeguarded to sustain or advance the DoD technological lead in the warfighter's battle space or joint operational arena. | -Sustain or advance DoD technological lead |
| The Critical Program Information (CPI), if compromised, will significantly alter program direction; result in unauthorized or inadvertent disclosure of the program or system capabilities; shorten the combat effective life of the system; or require additional research, development, test, and evaluation resources to counter the impact of its loss. | - Unauthorized disclosure of program or system capabilities<br>- Require additional RDT&E to counter loss |
| The theft or misappropriation of U.S. proprietary information or trade secrets, especially to foreign governments and their agents, directly threatens the economic competitiveness of the U.S. economy. Increasingly, foreign governments, through a variety of means, actively target U.S. businesses, academic centers, and scientific developments to obtain critical technologies and thereby provide their own economies with an advantage. Industrial espionage, by both traditionally friendly nations and recognized adversaries, proliferated in the 1990s and has intensified with computer network attacks today. | - Implies proprietary info may be included |

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| Information that may be restricted and protected is identified, marked, and controlled in accordance with DoD Directives 5230.24 and 5230.25 or applicable national-level policy and is limited to the following: | |
| • Information that is classified in accordance with Executive Order 13526, and | |
| • Unclassified information that has restrictions placed on its distribution by: | |
| • U.S. Statutes (e.g., Arms Export Control Act, Export Administration Act); | |
| • Statute-driven national regulations (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR)); and | |
| • Related national policy (e.g., Executive Order 13526, National Security Decision Directive 189). | |
| • 13.3.1.1 Critical Program Information (CPI) Identification | |
| Critical Program Information (CPI) determination is done with decision aids and Subject Matter Experts (SMEs). As general guidance, program managers should identify an element or component as Critical Program Information (CPI) if: | |

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| • Critical technology components will endure over its lifecycle | - Endure over its lifecycle (implies persistence) |
| • A critical component which supports the warfighter is difficult to replace | |
| • A capability depends on technology that was adjusted/adapted/calibrated during testing and there is no other way to extrapolate usage/function/application | - Calibrated during testing, no other way to extrapolate usage/function/application |
| • The component/element was identified as Critical Program Information (CPI) previously and the technology has been improved or has been adapted for a new application | - Previously identified as CPI and has been improved or adapted for new application |
| • The component/element contains a unique attribute that provides a clear warfighting advantage (i.e. automation, decreased response time, a force multiplier) | - Unique attribute providing clear warfighting advantage |
| • The component/element involves a unique method, technique, application that cannot be achieved using alternate methods and techniques | - Unique method, technique, aplication |
| • The component/element's performance depends on a specific production process or procedure | - Unique production process |
| • The component/element affords significant operational savings and/or lower operational risks over prior doctrine, organization, training, materiel, leadership and education, personnel, | |

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| • Critical technology components will endure over its lifecycle | - Endure over its lifecycle (implies persistence) |
| • A critical component which supports the warfighter is difficult to replace | |
| • A capability depends on technology that was adjusted/adapted/calibrated during testing and there is no other way to extrapolate usage/function/application | - Calibrated during testing, no other way to extrapolate usage/function/application |
| • The component/element was identified as Critical Program Information (CPI) previously and the technology has been improved or has been adapted for a new application | - Previously identified as CPI and has been improved or adapted for new application |
| • The component/element contains a unique attribute that provides a clear warfighting advantage (i.e. automation, decreased response time, a force multiplier) | - Unique attribute providing clear warfighting advantage |
| • The component/element involves a unique method, technique, application that cannot be achieved using alternate methods and techniques | - Unique method, technique, aplication |
| • The component/element's performance depends on a specific production process or procedure | - Unique production process |
| • The component/element affords significant operational savings and/or lower operational risks over prior doctrine, organization, training, materiel, leadership and education, personnel, | |

# Defense Acquisition Guidebook (DAG), 10/9/12

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| • and facilities (DOTMLPF) methods | |
| • The Technology Protection and/or Systems Engineering (SE) Team recommends that the component/element is identified as Critical Program Information (CPI) | |
| • The component/element will be exported through Foreign Military Sales (FMS)/Direct Commercial Sales (DCS) or International Cooperation | - Element will be exported |
| PMs should contact their Component research and development acquisition protection community for assistance in identifying Critical Program Information (CPI). | |
| | |

# NDIA Proposed CPI Definition

| Definition | Summary Statements Useful for ID'ing CPI |
|---|---|
| CPI. DoD-unique or leading-edge elements of a military-relevant system that, if compromised, could cause significant degradation in mission effectiveness or reduce technological advantage. Compromise means allowing an adversary to see the CPI (sight sensitive, also known as *confidentiality*), modify the CPI (modification sensitive, also known as *integrity*), or test the performance of the system or component (performance sensitive). | -DoD Unique or leading edge elements of a military relevant system<br>- Significant degradation in mission effectiveness<br>- Reduced technological advantage<br>- sight, modification, performance sensitive |
| Discussion: | |
| CPI may exist at the component, subsystem, or system level. CPI may manifest itself in the form of information (e.g., technical designs, performance characteristics), technology (e.g., manufacturing processes, algorithms), or components (e.g., hardware, software, firmware, data). The integrated whole system may itself be CPI, in that compromise may allow the system to be copied and provide an adversary with a military capability not otherwise available. Protections themselves may be CPI, if compromise of those protections could lead to the compromise of the CPI it is protecting. | - Component, subsystem, system level<br>- Information, technology, components<br>- Integrated whole<br>- Protections |
| Includes information about applications, capabilities, processes, and end-items. Includes classified information and operational data. | - Information about capabilities, processes, end-items<br>- Classified information<br>- Operational data |
| CPI does *not* include publically available information, or Commercial Off-the-Shelf (COTS) technologies or information otherwise protected by USG controls, such as ITAR/EAR. | - Not COTS, public data, ITAR |
| CPI shall be identified early in the research, technology development and acquisition processes, but no later than Milestone B or equivalent (Identify candidates by Milestone A). | |

# NDIA Proposed CPI Definition

| **Definition** | **Summary Statements Useful for ID'ing CPI** |
|---|---|
| Pre-systems acquisition and acquisition programs shall review their programs for CPI when technologies are transitioned from research and development or inherited from another program, during the technology development phase, throughout a program's life cycle, and as directed by the MDA.  RFPs and contracts should require identification of CPI inherited from other programs, as well as whether the developing government organization deems it as adequately protected. | - Inherited CPI |
| CPI should be removed from the program's CPI list if it no longer meets the criteria above. | |
| CPI is owned by the originating program.  If a different program wants to re-use that CPI, they are responsible for ensuring horizontal protection, and should coordinate with the originating program in transitioning the technology. | |

# Election Results 2013 (Establishing "Truth")

## Summit Truth* - Green, CPI; Red, not CPI (by vote)

| # | Candidate Critical Program Information (CPI) | Yes | No | Gov't Yes | Gov't No | Industry Yes | Industry No | CPI Participant Yes | CPI Participant No |
|---|---|---|---|---|---|---|---|---|---|
| 🟢 1 | Tracker algorithm developed under IRAD, high performance, unique. Compromise could lead to development of countermeasures | 25 | 1 | 11 | 0 | 13 | 1 | 18 | 0 |
| 🟢 2 | Signal processing algorithm regarded as CPI by another program and protected by that program with technical countermeasures | 25 | 2 | 12 | 0 | 12 | 2 | 16 | 2 |
| 🔴 CLOSE 3 | UAV Operational data: waypoints (classified) | 11 | 15 | 6 | 6 | 5 | 9 | 7 | 10 |
| 🟢 CLOSE 4 | Operational data: target location data | 11 | 15 | 7 | 5 | 4 | 10 | 7 | 10 |
| 🟢 5 | Anti-Tamper know-how and design information | 22 | 5 | 10 | 2 | 11 | 3 | 15 | 3 |
| 🟢 6 | ECCM performance, classified by program SCG | 17 | 9 | 6 | 5 | 10 | 4 | 13 | 4 |
| 🔴 7 | Weapon accuracy (Circular Error Probable, CEP), classified by program SCG | 9 | 18 | 3 | 9 | 5 | 9 | 7 | 11 |
| 🟢 8 | Simulation operated by prime and government accurately predicting classified performance | 17 | 8 | 8 | 2 | 8 | 6 | 11 | 5 |
| 🟢 9 | System has export license proviso requiring AT to prevent modification of Operational Flight Program that could increase capability approved for release. Would not otherwise qualify as CPI. | 17 | 10 | 10 | 2 | 6 | 8 | 12 | 6 |
| 🟢 10 | COMSEC keys for operational data link | 19 | 8 | 10 | 2 | 8 | 6 | 12 | 6 |
| 🟢 11 | T/R Module (not COTS) that breaks 5230.28 threshold | 25 | 0 | 11 | 0 | 13 | 0 | 16 | 0 |
| 🟢 12 | Fire control minimum detectable target RCS (breaks 5230.28 threshold), classified by SCG | 19 | 7 | 8 | 3 | 10 | 4 | 13 | 4 |

* "Summit Truth" relies on weighting government votes at 80% and CPI participants 20%. Items labeled as "close" were within the 45-55% band of the weighted average.

# Election Results 2013

Summit Truth

| # | Candidate Critical Program Information (CPI) | Yes | No | Gov't Yes | Gov't No | Industry Yes | Industry No | CPI Participant Yes | CPI Participant No |
|---|---|---|---|---|---|---|---|---|---|
| 🔴 13 | Fire control minimum detectable target RCS (does NOT break 5230.28 threshold), classified by SCG | 10 | 16 | 4 | 7 | 5 | 9 | 8 | 9 |
| 🟢 14 | Software prevented from export by license proviso, but not otherwise meeting CPI criteria | 13 | 14 | 8 | 4 | 5 | 9 | 9 | 9 |
| 🟢 15 | Tracker algorithm developed under proprietary IRAD, high performance, unique. | 22 | 5 | 10 | 2 | 11 | 3 | 17 | 1 |
| 🟢 CLOSE 16 | GPS keying material | 14 | 11 | 6 | 5 | 8 | 5 | 9 | 7 |
| 🟢 17 | Weapon system providing unique performance in the world, but not containing otherwise identifiable CPI | 15 | 9 | 7 | 4 | 7 | 5 | 13 | 4 |
| 🔴 18 | New component offering significant reduction in cost or reduced maintenance, but not in performance | 5 | 22 | 3 | 9 | 2 | 12 | 4 | 14 |
| 🟢 19 | Unique manufacturing process providing element/component a military advantage | 22 | 5 | 11 | 1 | 10 | 4 | 15 | 3 |
| 🟢 20 | Signal processing algorithm regarded as CPI by another program, unprotected | 20 | 6 | 9 | 2 | 10 | 4 | 12 | 5 |
| 🔴 21 | Weapon CEP, NOT classified by program SCG | 5 | 22 | 3 | 9 | 1 | 13 | 3 | 15 |
| 🔴 22 | COTS FPGA | 0 | 25 | 0 | 10 | 0 | 14 | 0 | 16 |
| 🔴 23 | Algorithm that would not otherwise qualify as CPI, but is being exported | 2 | 25 | 1 | 11 | 1 | 13 | 1 | 17 |
| 🔴 24 | Inertial Measurement Unit in exported weapon system designated as ITAR, COTS, not otherwise CPI | 3 | 23 | 2 | 9 | 1 | 13 | 1 | 16 |

# Election Results 2013

Summit Truth

| # | Candidate Critical Program Information (CPI) | Yes | No | Gov't Yes | Gov't No | Industry Yes | Industry No | CPI Participant Yes | CPI Participant No |
|---|---|---|---|---|---|---|---|---|---|
| ● 25 | Algorithm previously identified as CPI, but reduced in capability for export within a product with no other CPI. No longer provides technological advantage or degrades mission effectiveness. | 7 | 19 | 3 | 8 | 3 | 11 | 6 | 11 |
| ● 26 | COTS MMIC that breaks DoDI-S-5230.28 threshold | 8 | 17 | 4 | 7 | 4 | 9 | 6 | 11 |
| ● 27 | T/R Module (not COTS) that does NOT break 5230.28 threshold | 5 | 21 | 3 | 8 | 1 | 13 | 2 | 15 |
| ● 28 | Anti-Tamper, as implemented in final form in specific weapon system | 11 | 16 | 4 | 8 | 7 | 7 | 9 | 9 |
| ● 29 | Item on MCTL, but otherwise does not meet definition of CPI | 4 | 23 | 2 | 10 | 1 | 13 | 4 | 14 |

# CPI Test Vector: Evaluation

## Comparison of How Each Definition Compares to "Truth"

| | Candidate Critical Program Information (CPI) | CPI Class | Summit Truth | Current 5200.39[1] | Reason | Current 5200.39 & DAG[2] | Reason | Proposed NDIA Definition[3] | Reason |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Tracker algorithm developed under IRAD,high performance, unique. **Compromise could lead to development of countermeasures** | Tech Lead, CM | Y | Y | Could cause significant degradation in mission effectiveness (countermeasures) | Y | | Y | Technology advantage and susceptibilitly to countermeasures |
| 2 | Signal processing algorithm regarded as CPI by another program and protected by that program with technical countermeasures | Horiz Prot | Y | Y | | Y | | Y | |
| 3 | UAV Operational data: waypoints (classified) | Operational | N | N | | N | Will not endure over its lifecycle | Y | DoD-unique; classified; operational data |
| 4 | Operational data: target location data | Operational | Y | N | | N | Will not endure over its lifecycle | Y | DoD-unique; classified; operational data |
| 5 | Anti-Tamper know-how and design information | Protection | Y | Y | | Y | | Y | Protections that could lead to compromise of CPI it is protecting |
| 6 | ECCM performance, classified by program SCG | CM | Y | Y | | Y | | Y | Significant degradation in mission effectiveness |
| 7 | Weapon CEP, classified by program SCG | Performance | N | Y | Information about capabilities and end-items. | Y | Disclosure of the system capabilities | Y | includes classified information |
| 8 | Simulation operated by prime and government accurately predicting classified performance | Simulations | Y | Y | Information about capabilities and end-items. | Y | | Y | Classified |

- **Comparison of the CPI criteria of the 5200.39 CPI definition alone, 5200.39 plus DAG, and proposed NDIA definition. Ambiguities are resolved to a "no" determination. To be declared "yes," the candidate must clearly meet the CPI definition.**

# CPI Test Vector: Evaluation (Continued)

| | Candidate Critical Program Information (CPI) | CPI Class | Summit Truth | Current 5200.39[1] | Reason | Current 5200.39 & DAG[2] | Reason | Proposed NDIA Definition[3] | Reason |
|---|---|---|---|---|---|---|---|---|---|
| 10 | COMSEC keys for operational data link | COMSEC keys | Y | Y | Could cause significant degradation in mission effectiveness (countermeasures) | N | Will not endure over its lifecycle | Y | includes operational data |
| 11 | T/R Module (not COTS) that breaks 5230.28 threshold | 5230 | Y | N | May reduce technological advantage. Ambiguous. | Y | Unique warfighter advantage | Y | Reduces technological advantage |
| 12 | Fire control minimum detectable target RCS (breaks 5230.28 threshold), classified by SCG | 5230 | Y | N | information about capabilities and end-items. Ambiguous. | Y | Disclosure of the system capabilities | Y | Includes classified information. |
| 13 | Fire control minimum detectable target RCS (does NOT break 5230.28 threshold), classified by SCG | Performance | N | N | information about capabilities and end-items. | Y | Disclosure of the system capabilities | Y | Los of mission effectiveness; classified information |
| 14 | Software prevented from export by license proviso, but not otherwise meeting CPI criteria | Provisos | Y | N | No mention of provisos in CPI definition | Y | Yes but for the wrong reason. Any element exported is CPI. (General guidance) No mention of provisos | N | No mention of provisos. |
| 15 | Tracker algorithm developed under proprietary IRAD,high performance, unique. | Proprietary | Y | N | Ambiguous. Nothing in the definition explicitly makes this CPI. Possibly "elements critical to a military system or network mission" | N | Ambiguous. Proprietary theft is discussed, but not explicitly described as CPI. If it provides a clear warfighting advantage, would be CPI. CPI If uniqueness provides clear warfighter advantage, or cannot be achieved using other techniques. | Y | Technology advantage and susceptibilitly to countermeasures |

# CPI Test Vector: Evaluation (Continued)

| | Candidate Critical Program Information (CPI) | CPI Class | Summit Truth | Current 5200.39[1] | Reason | Current 5200.39 & DAG[2] | Reason | Proposed NDIA Definition[3] | Reason |
|---|---|---|---|---|---|---|---|---|---|
| 16 | GPS keying material | COMSEC keys | Y | N | Ambiguous. Not clear | N | Will not endure over its lifecycle | Y | includes operational data |
| 17 | Weapon system providing unique performance in the world, but not containing otherwise identifiable CPI | Performance | Y | N | Not an RDA component or element of an RDA program, but the final integrated end item | N | Integrated whole system; compromise would provide adversary a unique capability. CPI if the component/element contains a unique attribute that provides a clear warfighter advantage; entire system is not a component/element | Y | Integrated whole weapon system is CPI, compromise may allow system to be copied and provide adversary with military capability not otherwise available. |
| 18 | New component offering significant reduction in cost or reduced maintenance, but not in performance | Cost | N | N | | N | | N | |
| 19 | Unique manufacturing process providing element/component a military advantage | Manufacturing | Y | Y | | Y | | Y | |
| 20 | Signal processing algorithm regarded as CPI by another program, unprotected | Horiz Prot | Y | Y | CPI inherited from another program is CPI | Y | | Y | Must coordinate with other program, protect to same level (in this case, unprotected) |

# CPI Test Vector: Evaluation (Continued)

| | Candidate Critical Program Information (CPI) | CPI Class | Summit Truth | Current 5200.39[1] | Reason | Current 5200.39 & DAG[2] | Reason | Proposed NDIA Definition[3] | Reason |
|---|---|---|---|---|---|---|---|---|---|
| 21 | Weapon CEP, NOT classified by program SCG | Performance | N | Y | information about capabilities and end-items. | Y | Disclosure of the system capabilities | N | No, if publically avaialble. Would not lead to loss of mission effectiveness or technological advantage due to lack of classification. |
| 22 | COTS FPGA | COTS | N | Y | Includes elements critical to a military system or network mission | N | Ambiguous. Yes if risk of manipulation is high. | N | COTS excluded |
| 23 | Algorithm that would not otherwise qualify as CPI, but is being exported | Export | N | N | | Y | If exported, as general guidance, it is CPI | N | |
| 24 | Intertial Measurement Unit in exported weapon system designated as ITAR, COTS, not otherwise CPI | ITAR | N | N | | Y | If exported, as general guidance, it is CPI. | N | COTS excluded, ITAR excluded |
| 25 | Algorithm previously identified as CPI, but reduced in capability for export within a product with no other CPI. No longer provides technological advantage or degrades mission effectiveness. | Horiz Prot | N | N | | Y | Previously identified CPI and adapted for a new application is CPI (general guidance). | N | |
| 26 | COTS MMIC that breaks DoDI-S-5230.28 threshold | COTS, 5230 | N | N | Ambiguous. May be critical to a military system or network mission. | N | Ambiguous. Yes if risk of manipulation is high. | N | COTS excluded |
| 27 | T/R Module (not COTS) that does NOT break 5230.28 threshold | Performance | N | N | Ambiguous. May reduce technological advantage | N | If not unique in the world | N | Does not compromise technological advantage |
| 28 | Anti-Tamper, in final form in specific weapon system, as seen by adversary (no know-how) | Protection | N | N | | N | | N | |
| 29 | Item on MCTL, but otherwise does not meet definition of CPI | Performance | N | N | | N | No reference to MCTL in definition or DAG. | N | No reference to MCTL |