System Security Engineering for Program Protection and Cybersecurity

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

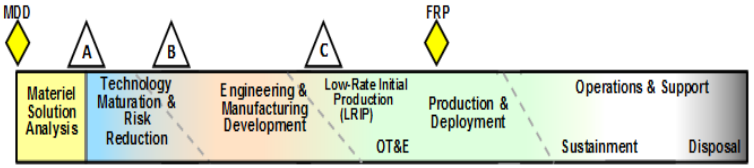
18th Annual NDIA Systems Engineering Conference

Springfield, VA | October 27, 2015

Ensuring Confidence in Defense Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter US capability
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled defense information resident on, or transiting supply chain networks
  - Loss or sale of US capability that provides a technological advantage
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact
  - Loss of US capability that provides a technological advantage

Access points are throughout the acquisition lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Spectrum of Program Protection Risks to Consider

Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.

Reverse Engineering

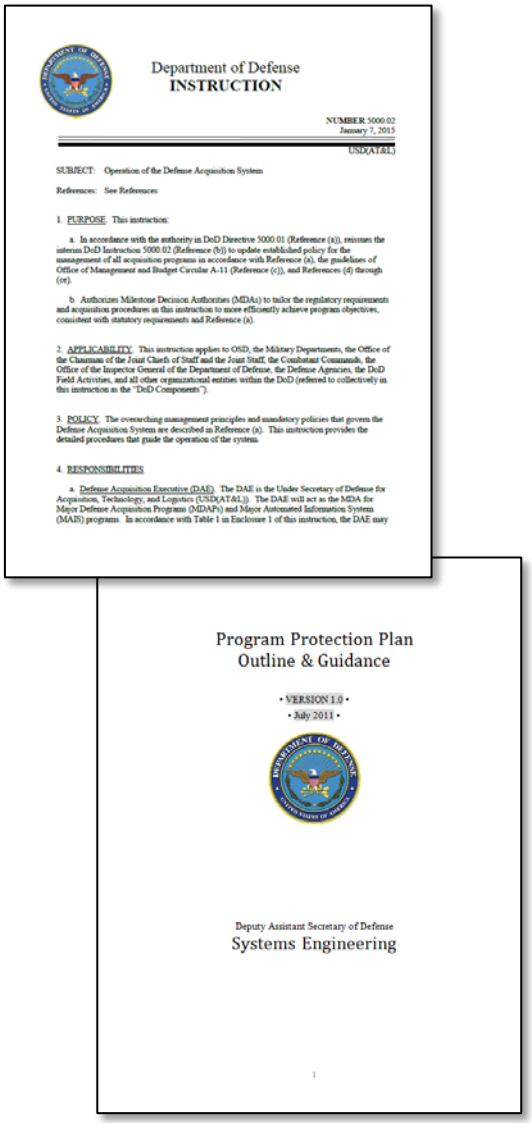
Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors

Program Protection in DoDI 5000.02


Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See References

1. PURPOSE. This instruction:

a. In accordance with the authority in DoD Directive 5000.01 (Reference (a)), reissues the interim DoD Instruction 5000.02 (Reference (b)) to update established policy for the management of all acquisition programs in accordance with Reference (a), the guidelines of Office of Management and Budget Circular A-11 (Reference (c)), and References (d) through (ee).

b. Authorizes Milestone Decision Authorities (MDAs) to tailor the regulatory requirements and acquisition procedures in this instruction to more efficiently achieve program objectives, consistent with statutory requirements and Reference (a).

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

3. POLICY. The overarching management principles and mandatory policies that govern the Defense Acquisition System are described in Reference (a). This instruction provides the detailed procedures that guide the operation of the system.

4. RESPONSIBILITIES.

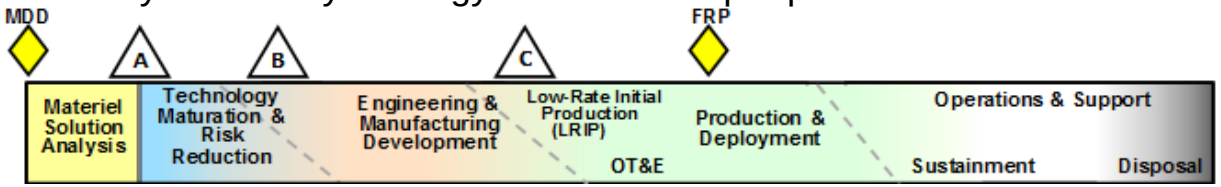
a. Defense Acquisition Executive (DAE). The DAE is the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)). The DAE will act as the MDA for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) programs. In accordance with Table 1 in Enclosure 1 of this instruction, the DAE may

Program Protection Plan
Outline & Guidance

• VERSION 1.0 •
• July 2011 •

Deputy Assistant Secretary of Defense
Systems Engineering

- **DoD considers SSE a critical discipline of SE. To further establish SSE, DoD has focused on integrating SSE into SE policy, contracts and workforce education.**
- **System Security Engineering is accomplished in the DoD through program protection planning (PPP)**
- **DoDI 5000.02 requires program managers to employ system security engineering practices and prepare a Program Protection Plan to manage the security risks to critical program information, mission-critical functions and information**
- **Program managers will describe in their PPP:**
  - Critical Program Information, mission-critical functions and critical components, and information security threats and vulnerabilities
  - Plans to apply countermeasures to mitigate associated risks
  - Plans for exportability and potential foreign involvement
  - The Cybersecurity Strategy and Anti-Tamper plan are included



Program Protection Integrated in Policy

DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD

DoDI 5200.39 Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Rescoped definition of CPI

DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components

DoDI 4140.67 DoD Counterfeit Prevention Policy

- Establishes policy and assigns responsibility to prevent the introduction of counterfeit material at any level of the DoD supply chain

DoDI 8500.01 Cybersecurity

- Establishes policy and assigns responsibilities to achieve DoD cybersecurity through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

What Are We Protecting?

Program Protection Planning
DoDI 5000.02

DoDM 5200.01, Vol. 1-4 | DoDM 5200.45 | DoDI 8500.01

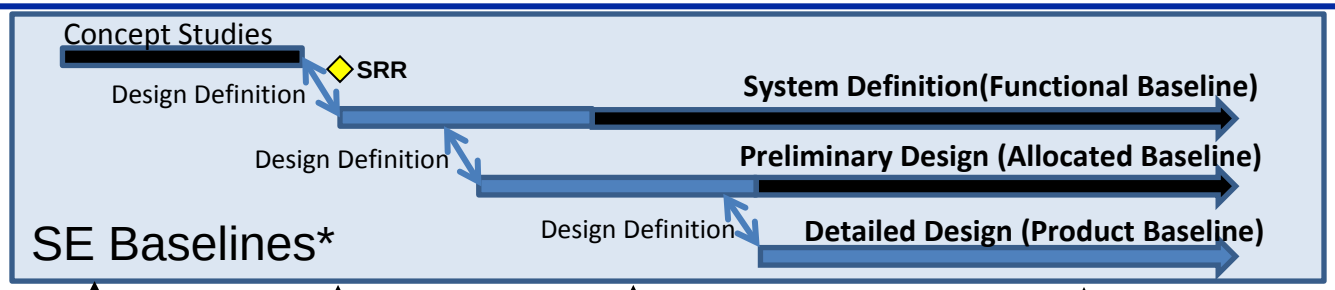
DoDI 5200.39 | DoDI 5200.44 | DoDI 5230.24 | DoDI 8510.01

Technology	Components	Information
What: A capability element that contributes to the warfighters' technical advantage (CPI)	What: Mission-critical elements and components	What: Information about applications, processes, capabilities and end-items
Who Identifies: System Engineers with CI/Intel and Security SME support	Who Identifies: System Engineers, Logisticians	Who Identifies: All
ID Process: CPI Identification	ID Process: Criticality Analysis	ID Process: CPI identification, criticality analysis, and classification guidance
Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence (CI) assessments	Threat Assessment: Defense Intelligence Agency Threat Analysis Center	Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments
Countermeasures: Anti-Tamper, Classification, Exportability Features, Security, etc.	Countermeasures: SCRM, Cybersecurity, Anti-counterfeits, software assurance, Trusted Foundry, etc.	Countermeasures: Cybersecurity, Classification, Export Controls, Security, etc.
Goal: "Keep secret stuff in" by preventing the compromise and loss of CPI	Goal: "Keep malicious stuff out" by protecting key mission components	Goal: "Keep critical information from getting out" by protecting data from our adversaries

Protecting Warfighting Capability Throughout the Lifecycle

Policies, guidance and white papers are found at our initiatives site: http://www.acq.osd.mil/se/initiatives/init_pp-sse.html

Systems Security Engineering Integrates Program Protection Planning



Protection measures are identified and integrated into technical baselines, iteratively informed by and informing the maturing design.

Criticality Analysis

- Determine critical components based on critical mission threads
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

CPI Analysis

- Identify capability elements providing a US technological advantage
- Assess the risk associated with each CPI (exposure, consequence of compromise)
- Conduct horizontal analysis

Cybersecurity

- Categorize system (C,I,A)
- Identify control baselines and overlays, then tailor
- Trace controls to requirements

Threats and Vulnerabilities Assessment

- Identify supply chain threats and vulnerabilities
- Identify foreign collection threats and vulnerabilities
- Identify personnel, physical, operational threats and vulnerabilities

Program Protection Plan

- Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/ software assurance, physical security, operations security, supply chain, system security, and trusted suppliers
- Determine foreign involvement expectations and impacts on protection measures
- Conduct engineering risk/cost trade-off analysis to select protection measures
- Identify acquisition mitigations (e.g., blind buy, trusted source)
- Determine system security requirements

Contractor

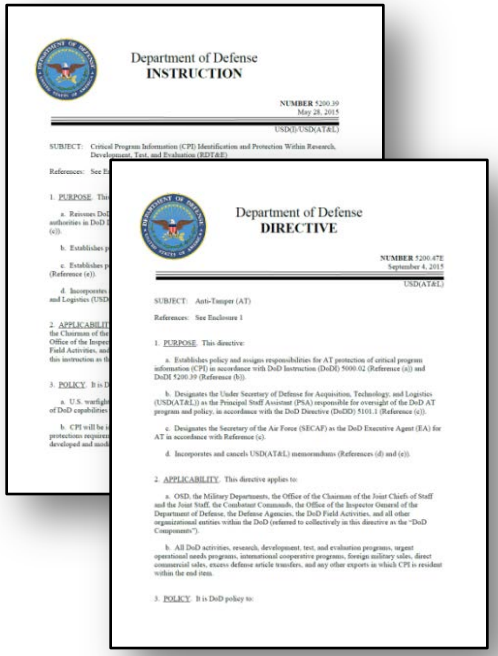
- Respond to acquisition and security requirements
- Continually assess security risks during design reviews and system implementation
- Conduct early defense exportability features planning and design

Test and Evaluation

- Assess hardware and software vulnerabilities
- Evaluate Anti-Tamper protections
- Verify security requirements (Contractor, DT&E, OT&E)

CPI Policy Updates

- **CPI and AT Policy Updates**
  - ***DoDI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E):*** Revises the CPI definition, requires CPI identification early and throughout the program, and emphasizes horizontal identification and protection
  - ***DoDD 5200.47E, Anti-Tamper:*** Designates the Secretary of the AF as the Executive Agent for Anti-Tamper and establishes requirements for AT planning, implementation, and evaluation.


Department of Defense
INSTRUCTION

Department of Defense
DIRECTIVE

- **Revised definition of CPI has been scoped to focus only on those elements that provide a capability advantage and reside on the end-item (system or supporting systems)**
  - "U.S. capability elements that contribute to the warfighters' technical advantage, which if compromised, undermines U.S. military preeminence. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the system, its training equipment, or maintenance support equipment."

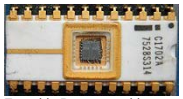
Joint Federated Assurance Center (JFAC)

Field Programmable Gate Array

Binary Computer Software Code

```
static void goodG2B() { char * data;
char data_buf[100] = ""; data =
data_buf; /* FIX: Specify the full
pathname for the library */
strcpy(data,
"C:\\Windows\\System32\\winsrv.dl
l"); { HMODULE hModule; /*
POTENTIAL FLAW: If the path to
the library is not specified, an
attacker may be able to * replace
his own file with the intended
library */ hModule =
LoadLibrary(data); if (hModule !=
NULL) { FreeLibrary(hModule);
printLine("Library loaded and freed
successfully"); } else { /*
printLine("Unable to load library");
} } }
```

Computer Source Software Code



Erasable Programmable Read-Only Memory (EPROM)

Assure Mission SW and HW Security

Intent:

- Congress directed DoD to "…*provide for the establishment of a joint federation of capabilities to support the trusted defense system needs…to ensure security in the software and hardware developed, acquired, maintained, and used by the Department*." (FY14 NDAA, Sect. 937)

Expected Outcomes/Deliverables:

- Federated cross-DoD awareness and coordination of software and hardware assurance (SwA/HwA) capabilities and expertise
- Development and sharing of SwA/HwA vulnerability assessment best practices, tested tools, and proven processes
- Identification of R&D needs to advance SwA/HwA capabilities for programs in acquisition, operational systems, and legacy systems and infrastructure

Key Participants:

- Sponsor(s): ASD(R&E)/DASD(SE)
- Contributors: CIO, AF, Army, Navy, USMC, NSA, NRO, MDA, DISA, Defense Microelectronics Activity (DMEA)

Approach:

- Establish federation of HwA and SwA capabilities to support programs in program protection planning and execution
- Support program offices across life cycle by identifying and facilitating access to Department SwA and HwA expertise and capabilities, policies, guidance, requirements, best practices, contracting language, training, and testing support
- Coordinate with DoD R&D for HwA and SwA
- Procure, manage, and distribute enterprise licenses for SwA/HwA tools

Milestones:

Formed Steering Committee and Working Groups	7/14
Initiated First Series of Technical Tasks	9/14
Charter signed by Deputy Secretary of Defense	2/15
Congressional Report on funding, organization, management, and operations of JFAC signed & submitted	3/15
CONOPS signed by stakeholders of Federation	8/15
Capability Assessment, Gap Analysis, Strategic Plan	10/15
Joint Federated Assurance Center (JFAC) IOC	12/15

Program Protection Integrated in Contract Regulation

DFARS 252.204-7012

Purpose:
Establish minimum requirements for DoD unclassified controlled technical information on contractor information systems

Requires:
Contractors implement minimum set of information security controls

Flow Down to Subcontractors

Contractors report cyber incident and compromises on Controlled Technical Information

Contractor actions to support DoD damage assessment as needed

Published November 18, 2013

- **DFARS Subpart 204.73 – Safeguarding Unclassified Controlled Technical Information**
  http://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm#204.7303
- **PGI 204.7303-3 Cyber Incident and Compromise Reporting**
  http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/PGI204_73.htm#204.7303-3
- **DoDI 5230.2, Distribution Statements on Technical Documents**
  http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf
- **Frequently Asked Questions (FAQs) Regarding DFARS Subpart 204.73 and PGI Subpart 204.73**
  http://www.acq.osd.mil/dpap/pdi/docs/ControlledTechnicalInformation_FAQ.pdf
- **Guidance to Requiring Activities for Implementing DFARS Clause 252.204-7012, Safeguarding Unclassified Controlled Technical Information**
  http://www.acq.osd.mil/se/docs/DFARS-guide.pdf

****New Interim Rule Safeguarding of Covered Defense Information and Cyber Incident Reporting published in 2015:**

- Expands scope to covered defense information
- Direct the use in all solicitations and contracts
- Replaces security controls specified in NIST SP 800-53 with NIST SP 800-171
- Contractors to report cyber incidents affecting Controlled Defense Information and ability to provide operationally critical support
- Contractors to submit any malicious software

PPP Elements within Request For Proposal (RFP)

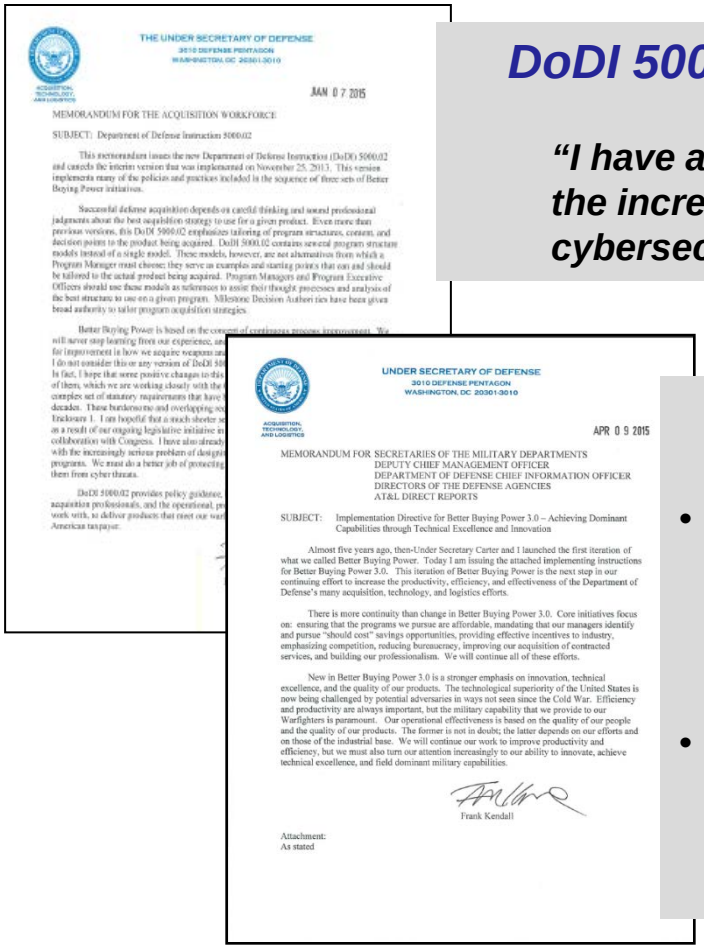
- **Review document titled, "*Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into DoD Requests For Proposals*"***

- **Statement of Work (SOW) Systems Engineering (SE) Section or Security Section**
  - Review and adapt statements from the "suggested language"*
  - At a minimum include SOW001, SOW004, SOW009 and SOW0010
    - These statements ensure that criticality analysis, supply chain risk, and software assurance are addressed by the contractor
- **Section L**
  - Include statement SECL0002 from "suggested language"*
    - This requires the contractor to describe the integration of program protection into their SE processes
- **Ensure that Systems Engineering Plan (SEP) Section 4.4 Technical Reviews include:**
  - Entry Criteria – Updated PPP (this will capture the CA/VA/TA activities)
  - Products – Updated Security Risk Assessment and Mitigation Plans; updated PP Activities on Program Schedule
- **If not included in the SEP then incorporate in the SOW an updated PPP as entrance criteria to all technical reviews and an updated risk assessment as an exit criteria for all technical reviews**

RFP/SOW Plays a Key Role in Integrating the PPP into SE

*http://www.acq.osd.mil/se/docs/SSE-Language-for-TSN-in-DoD-RFPs.pdf

Designing and Managing Cybersecurity in our Programs



THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

JAN 07 2015

MEMORANDUM FOR THE ACQUISITION WORKFORCE

SUBJECT: Department of Defense Instruction 5000.02

This memorandum issues the new Department of Defense Instruction (DoDI) 5000.02 and cancels the interim version that was implemented on November 25, 2013. This version implements many of the policies and practices included in the sequence of three sets of Better Buying Power initiatives.

Successful defense acquisition depends on careful thinking and sound professional judgments about the best acquisition strategy to use for a given product. Even more than previous versions, this DoDI 5000.02 emphasizes tailoring of program structures, content, and decision points to the product being acquired. DoDI 5000.02 contains several program structure models instead of a single model. These models, however, are not alternatives from which a Program Manager must choose; they serve as examples and starting points that can and should be tailored to the actual product being acquired. Program Managers and Program Executive Officers should use these models as references to assist their thought processes and analysis of the best structure to use on a given program. Milestone Decision Authorities have been given broad authority to tailor program acquisition strategies.

Better Buying Power is based on the concept of continuous process improvement. We will never stop learning from our experience, and [illegible] for improvement is how we acquire weapons and [illegible] I do not consider this or any version of DoDI 50[illegible] In fact, I hope that some positive changes to this [illegible] of them, which we are working closely with the [illegible] complex set of statutory requirements that have [illegible] decades. These burdensome and overlapping [illegible] Enclosure 1. I am hopeful that a much shorter [illegible] as a result of our ongoing legislative initiative in [illegible] collaboration with Congress. I have also already [illegible] with the increasingly serious problem of designing [illegible] programs. We must do a better job of protecting [illegible] them from cyber threats.

DoDI 5000.02 provides policy guidance, [illegible] acquisition professionals, and the operational, [illegible] work with, to deliver products that meet our war[illegible] American taxpayer.

UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

APR 09 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
DEPUTY CHIEF MANAGEMENT OFFICER
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
DIRECTORS OF THE DEFENSE AGENCIES
AT&L DIRECT REPORTS

SUBJECT: Implementation Directive for Better Buying Power 3.0 – Achieving Dominant Capabilities through Technical Excellence and Innovation

Almost five years ago, then-Under Secretary Carter and I launched the first iteration of what we called Better Buying Power. Today I am issuing the attached implementing instructions for Better Buying Power 3.0. This iteration of Better Buying Power is the next step in our continuing effort to increase the productivity, efficiency, and effectiveness of the Department of Defense's many acquisition, technology, and logistics efforts.

There is more continuity than change in Better Buying Power 3.0. Core initiatives focus on: ensuring that the programs we pursue are affordable, mandating that our managers identify and pursue "should cost" savings opportunities, providing effective incentives to industry, emphasizing competition, reducing bureaucracy, improving our acquisition of contracted services, and building our professionalism. We will continue all of these efforts.

New in Better Buying Power 3.0 is a stronger emphasis on innovation, technical excellence, and the quality of our products. The technological superiority of the United States is now being challenged by potential adversaries in ways not seen since the Cold War. Efficiency and productivity are always important, but the military capability that we provide to our Warfighters is paramount. Our operational effectiveness is based on the quality of our people and the quality of our products. The former is not in doubt; the latter depends on our efforts and on those of the industrial base. We will continue our work to improve productivity and efficiency, but we must also turn our attention increasingly to our ability to innovate, achieve technical excellence, and field dominant military capabilities.

Frank Kendall

Attachment:
As stated

DoDI 5000.02 Release Memo to the Acquisition Workforce

"I have also already initiated work on a new enclosure that will deal with the increasingly serious problem of designing for and managing cybersecurity in our programs."

Better Buying Power 3.0

- ***Develop a new Enclosure for DoDI 5000.02 addressing all aspects of the program manager's and other's responsibilities for cybersecurity throughout the product lifecycle. A draft will be provided to the USD(AT&L) by July 2015.***
- ***Review current system security engineering design processes and methods and recommend standardization or other approaches to improve cybersecurity of system designs, including all outside interfaces, by October 2015.***

Establishes expectations and provides methodology for SSE processes during design, development and through sustainment

Incorporating Program Protection into Acquisition Workforce Training

- **Effective program protection planning is enabled by qualified, trained personnel**
  - Two program protection courses are currently in development
  - First course (ENG 160) is expected to be available in FY16

- **ENG 160: Program Protection Overview**
  - Provides an overview of program protection concepts, policy and processes
  - Intended for the entire Acquisition Workforce, with focus on ENG and PM
- **ENG 260: Program Protection Practitioner Course**
  - Intended for Systems Engineers and System Security Engineers
  - Focuses on application of program protection concepts and processes

Our Focus on SSE and SE

- **DoD is putting guidance in place for a risk-based cost benefit trade-off process to protect programs and systems, their supply chain, and their software development**
- **DoD is emphasizing the importance of SSE within systems engineering and its contribution to the design of systems by:**
  - Ensuring that program protection is addressed as part of system engineering, test and sustainment activities
  - Incorporating program protection and system security engineering requirements and processes into engineering development contracts
  - Working with industry and standards groups to synergize methodologies
- **Industry has been playing an important role in the DoD SSE initiative by:**
  - Investing in research and processes to protect systems, the supply chain and the software development
  - Developing their SE and SSE processes and skills

DoD efforts are targeting integration of system security engineering considerations throughout the system life cycle

Systems Engineering: Critical to Defense Acquisition










Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se

For Additional Information

Melinda Reed

ODASD, Systems Engineering

571-372-6562 | Melinda.K.Reed4.civ@mail.mil

JeanPaul LeSaint

Engility Corporation

571-372-6554 | JeanPaul.R.LeSaint.ctr@mail.mil

Matthew Perticone

Engility Corporation

571-372-6555 | Matthew.Perticone.ctr@mail.mil

Example of NIST SP 800-53 Based Controls Mapped to NIST SP 800-171

Nov 2013 Safeguarding DFARS Table 1 (NIST SP 800-53 Requirement)	NIST SP 800-171 Req't
AC-2 ACCOUNT MANAGEMENT The organization: a. Identifies /selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. AC-3 ACCESS ENFORCEMENT The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. AC-17 REMOTE ACCESS The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.	3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Navigating Unclassified Cyber/Information (System) Security Protections

Elements that drive appropriate protections: The information system and the information

Contractor's Internal System

Applicable controls:
NIST SP 800-171

Contractor System Operated on DoD's Behalf

Applicable controls:
from CNSSI 1253,
based on NIST SP 800-53

Federal Contract Information

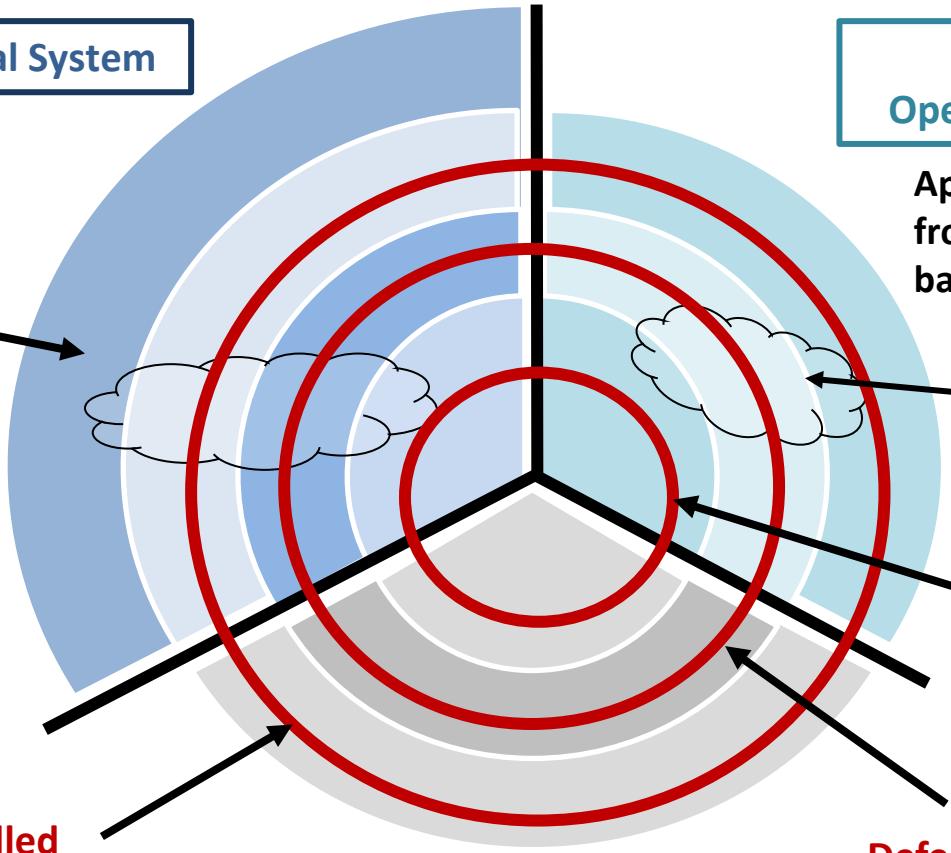
Cloud Service Provider

Applicable controls:
From the SRG

Unclassified Controlled Technical Information

Covered Defense Information

Controlled Unclassified Information (USG-wide)



DoD Information System

Applicable controls:
From CNSSI 1253, based on NIST SP 800-53

Network Penetration Reporting

DFARS subpart 204.73, Safeguarding of ~~Unclassified Controlled Technical~~ Covered Defense Information and Cyber Incident Reporting is modified to:

- Expands scope of safeguarding and reporting to covered defense information
- Direct the use of DFARS provision 252.204-7008 and DFARS clause 252.204-7012 in all solicitations and contracts
  - DFARS Clause 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls
  - DFARS Clause 252.204-7012, Safeguarding of ~~Unclassified Controlled Technical~~ Covered Defense Information and Cyber Incident Reporting
    - Replaces security controls based on NIST SP 800-53 with NIST SP 800-171
    - Requires contractors to report cyber incidents involving covered defense information as well as any cyber incident that may affect the ability to provide operationally critical support
    - Requires contractors to submit any malicious software that is discovered and isolated in connection with a reported cyber incident to DoD for analysis, and to allow DoD access to equipment in order to assess the magnitude of the loss or compromise of DoD information
- Direct use of DFARS Clause 252.204-7009, Limitations of Third-Party Contractor Information, in all solicitations/contracts for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.

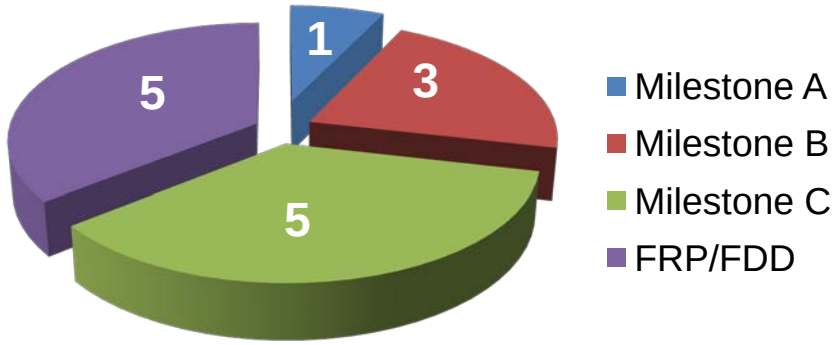
Expected Program Protection Analysis Maturity Throughout the Life Cycle

	ASR	SRR	SFR	PDR	CDR	SVR/FCA, P&D and O&S Phases
System Spec Level	• ICD / Comments on Draft CDD (if avail) • Prelim System Performance Spec • Notional sys model/ arch including CONOPS, i/f, & operational/ functional requirements	• System Performance Spec • Verifiable sys req'ts detailed to enable functional decomposition • Req. traceability • External i/f documented	• Functional Baseline • System functions decomposed and mapped to System elements • Sys elements defined • Preliminary allocation of functions optimized	• Allocated Baseline • Preliminary design (fct and i/f) for all elements (HW & SW) complete • HW – Verifiable component characteristics • SW – CSCs, CSUs	• Initial Product Baseline • Detailed design & i/f for comp/unit production and test • HW– Physical (form fit, function) • SW– CSU level design	• Product Baseline
Criticality Analysis (CA)	Mission-based functions	System requirements level functions	Subsystem level sub-functions	Assembly/ component	Component/ part	Part (prelim)
Vulnerability Assessment (VA)	• Response to Milestone A Vulnerability Questionnaire	• Vulnerability Questionnaire and Vulnerability DB assessment	• Vulnerability assessment for critical subsystems	• Vulnerability assessment for critical assemblies/ component s	• Vulnerability assessments, static analysis & diversity assessment to critical component level	• Vulnerability assessments, static analysis & diversity assessment to critical part level
Risk Assessment (RA)	• Objective risk criteria established • Applied at function level	• Risk criteria updated • applied at system level	• Risk criteria updated & applied at subsystem level	• Risk criteria updated & applied at assembly level	• Risk criteria updated & applied at component level	• Risk criteria updated & applied at part level of critical components
Counter-measure (CM)	• Risk based supply chain, design & SW CM selected via trade-off study	• Risk based system function level CM selection	• Risk based subsystem function level CM refinement & selection	• Risk based assembly level CM selection	• Risk based component level CM selection	• Risk based part level CM selection
Cyber security	• System Categorization/Registration • Initial Cyber Security(CS) Controls & tailoring	• Risk based control strength of implementation determined	• CS Control trace to spec • Additional CS Controls tailoring/trades as CM if needed	• CS Control trace to spec • Additional CS Controls as CM if needed • CS enabled Components ID'd as CM	• CS controls incorporated traced to product baseline • Controls Assessed and discrepancies ID'd/categorized	• CS controls incorporated traced to product baseline • IAVM program established for CS control maintenance
RFP	• CM and CS controls incorporated into TMRR SOW and SRD		• CM and CS controls incorporated into EMD SOW and SRD		• CM and CS controls incorporated into Production SOW and SRD	

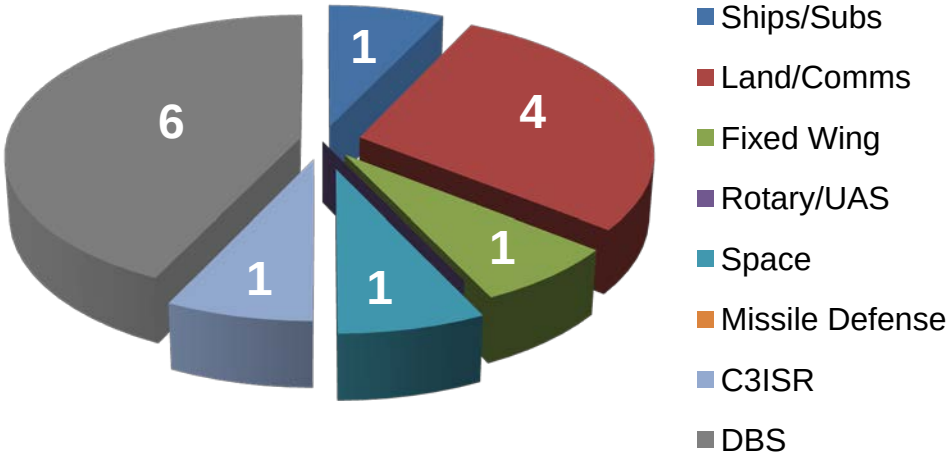
PPP Approval Statistics

63 PPPs Approved	
FY 2010 – 4	FY 2013 – 18
FY 2011 – 7	FY 2014 – 18
FY 2012 – 5	FY 2015 – 14

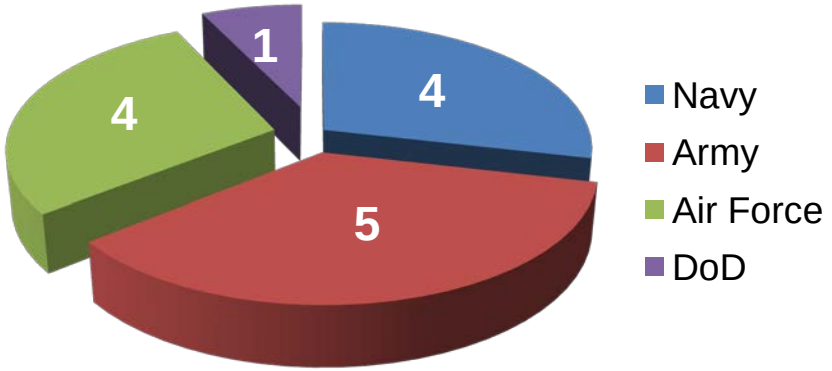
FY15 PPPs by Milestone



FY15 PPPs by Domain



FY15 PPPs by Service



Engaged with and tracked 50 programs during FY 2015