Integrating Cybersecurity into the Program Management Organization

Naval Postgraduate School Acquisition Symposium 2015

Panel #6

May 13, 2015

Erin M. Schultz,
The MITRE Corporation
eschultz@mitre.org

Virginia Wydler, CPCM, Fellow
The MITRE Corporation
vwydler@mitre.org

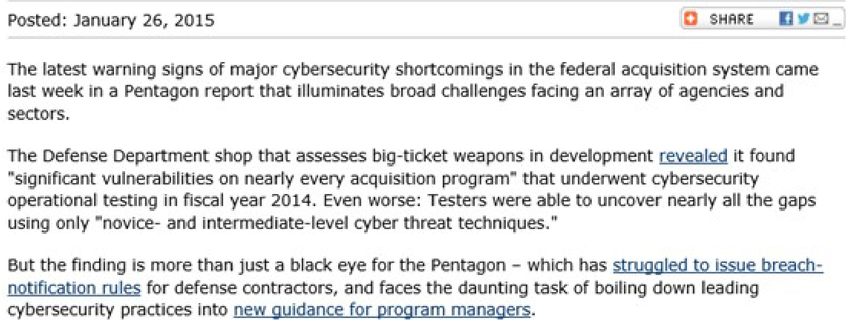
The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation. This document is approved for public release, 15-1454

Outline

- The Cybersecurity threat
- Laws, regulations, policy, and guidance
- Cybersecurity and the Program Manager
- Integrating Cyber into the Acquisition Lifecycle

Research Shows Cybersecurity is a Threat to our National Economy

DOD Cybersecurity Gaps Could Be Canary in Federal Acquisition Coal Mine



Posted: January 26, 2015

The latest warning signs of major cybersecurity shortcomings in the federal acquisition system came last week in a Pentagon report that illuminates broad challenges facing an array of agencies and sectors.

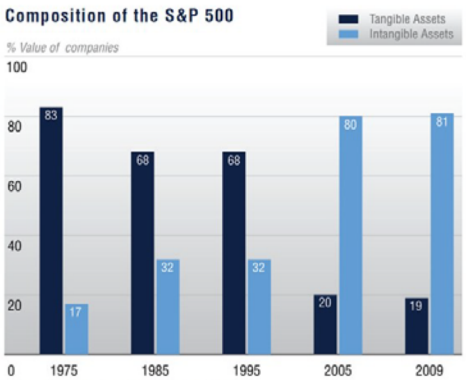
The Defense Department shop that assesses big-ticket weapons in development revealed it found "significant vulnerabilities on nearly every acquisition program" that underwent cybersecurity operational testing in fiscal year 2014. Even worse: Testers were able to uncover nearly all the gaps using only "novice- and intermediate-level cyber threat techniques."

But the finding is more than just a black eye for the Pentagon – which has struggled to issue breach-notification rules for defense contractors, and faces the daunting task of boiling down leading cybersecurity practices into new guidance for program managers.

Adversaries Outpace US In Cyber War; Acquisition Still Too Slow

By COLIN CLARK
on May 19, 2014 at 6:40 PM

Intangible Assets Create Vulnerabilities



Source: Ocean Tomo Intellectual Capital Equity.

- Intellectual capital rather than physical assets represents more than 80% of value of S&P 500, almost a flip from valuation in 1975
- Intangible assets far more susceptible to espionage
- "Criminals understand that there is much greater value in selling a company's proprietary information to competitors and foreign governments . . . the cyber underground economy has shifted its focus to the theft of corporate intellectual capital." - Simon Hunt, Vice President and Chief Technology Officer of McAfee, from 2011 report "Underground Economies"

Workplace and Personal Lives are Blurring

- 88% of companies offer smart devices (e.g., smart phone, PDA)
- 62% of companies enable remote desktop video conferencing
- 54% of companies use social media to engage workforce
- 46% of companies use cloud computing (and increasing)
- "By 2020, IT computing will be almost entirely outsourced to the Cloud, and the lines between business and personal technology will be blurred," - Richard Kadzis, VP, Strategic Communications, CoreNet Global

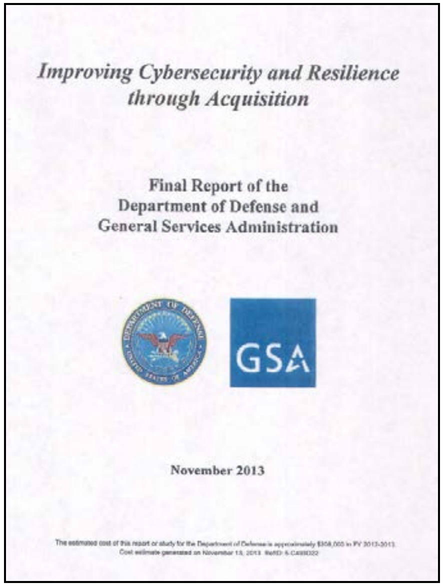
Source: http://www.channelinsider.com/c/a/Careers/How-Technology-Will-Change-the-Workplace-of-Tomorrow-333122/

Cybersecurity Guidance is Evolving

- **The Executive Branch identified cybersecurity as a serious economic and national security challenge**
  - DHS assigned primary responsibility for federal-wide information security program and compliance

Executive Order 13636: Improving Critical Infrastructure Cybersecurity February 2013

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February 2013



Improving Cybersecurity and Resilience through Acquisition

Final Report of the
Department of Defense and
General Services Administration

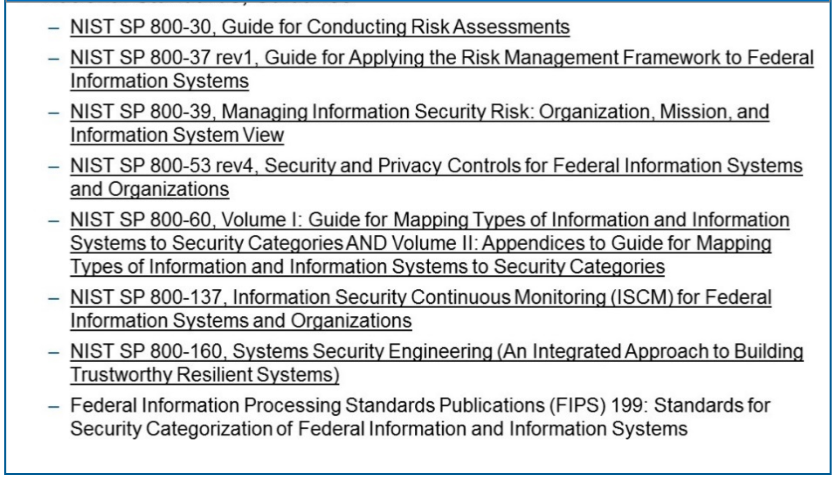
November 2013

The estimated cost of this report or study for the Department of Defense is approximately $308,000 in FY 2013-2013.
Cost estimate generated on November 13, 2013. RefID: [illegible]

Government's compelling drive is to better align cyber risk management and acquisition processes

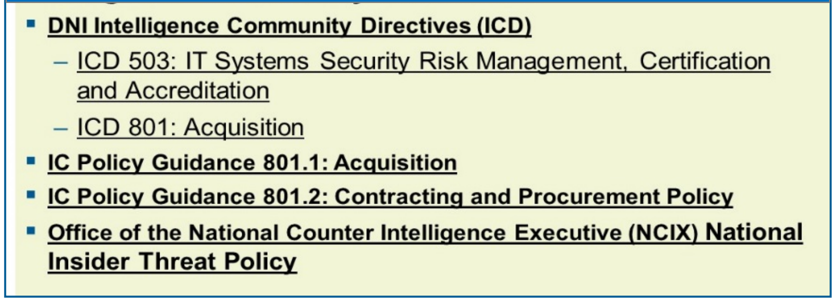
…With a Plethora of Existing References

National Standards, Guidance



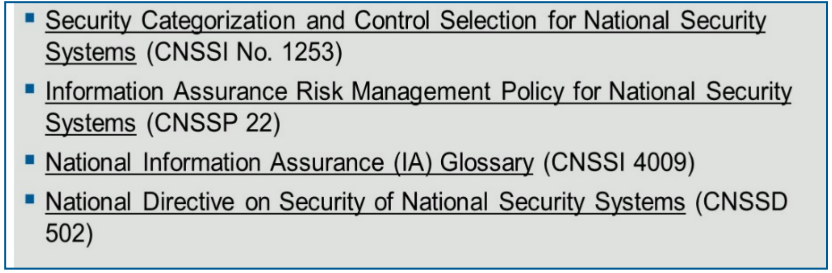
- NIST SP 800-30, Guide for Conducting Risk Assessments
- NIST SP 800-37 rev1, Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-53 rev4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories AND Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-160, Systems Security Engineering (An Integrated Approach to Building Trustworthy Resilient Systems)
- Federal Information Processing Standards Publications (FIPS) 199: Standards for Security Categorization of Federal Information and Information Systems

Intelligence Community



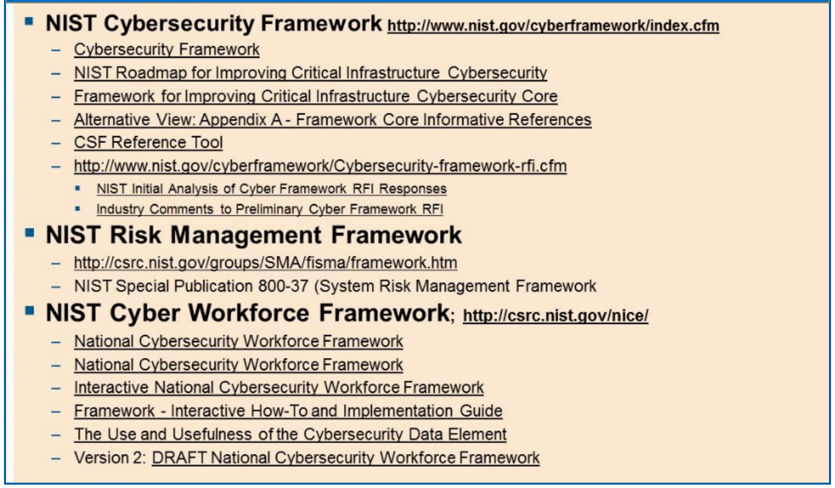
- **DNI Intelligence Community Directives (ICD)**
  - ICD 503: IT Systems Security Risk Management, Certification and Accreditation
  - ICD 801: Acquisition
- **IC Policy Guidance 801.1: Acquisition**
- **IC Policy Guidance 801.2: Contracting and Procurement Policy**
- **Office of the National Counter Intelligence Executive (NCIX) National Insider Threat Policy**

National Security System (NSS)



- Security Categorization and Control Selection for National Security Systems (CNSSI No. 1253)
- Information Assurance Risk Management Policy for National Security Systems (CNSSP 22)
- National Information Assurance (IA) Glossary (CNSSI 4009)
- National Directive on Security of National Security Systems (CNSSD 502)

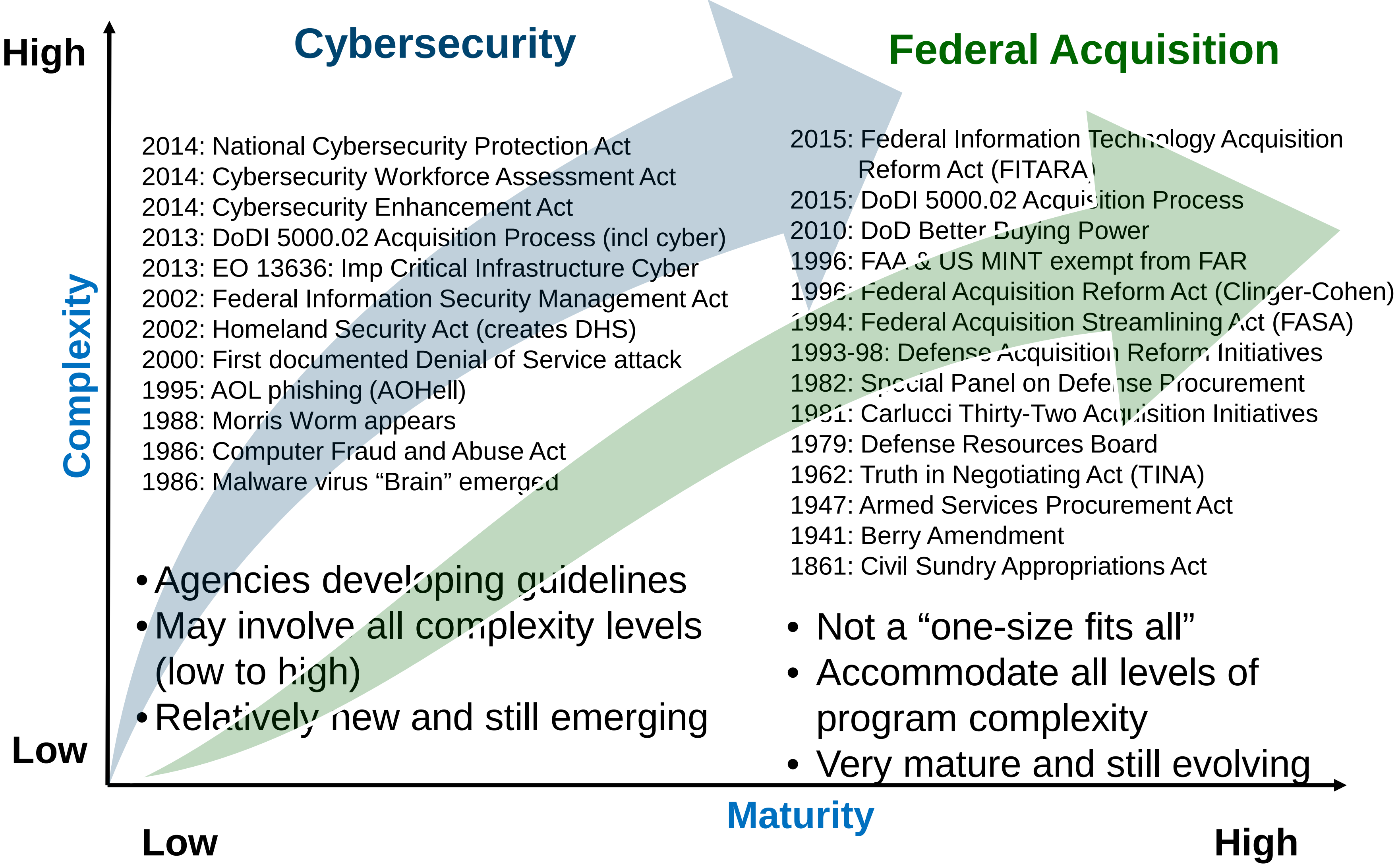
NIST Framework



- **NIST Cybersecurity Framework** http://www.nist.gov/cyberframework/index.cfm
  - Cybersecurity Framework
  - NIST Roadmap for Improving Critical Infrastructure Cybersecurity
  - Framework for Improving Critical Infrastructure Cybersecurity Core
  - Alternative View: Appendix A - Framework Core Informative References
  - CSF Reference Tool
  - http://www.nist.gov/cyberframework/Cybersecurity-framework-rfi.cfm
    - NIST Initial Analysis of Cyber Framework RFI Responses
    - Industry Comments to Preliminary Cyber Framework RFI
- **NIST Risk Management Framework**
  - http://csrc.nist.gov/groups/SMA/fisma/framework.htm
  - NIST Special Publication 800-37 (System Risk Management Framework
- **NIST Cyber Workforce Framework**; http://csrc.nist.gov/nice/
  - National Cybersecurity Workforce Framework
  - National Cybersecurity Workforce Framework
  - Interactive National Cybersecurity Workforce Framework
  - Framework - Interactive How-To and Implementation Guide
  - The Use and Usefulness of the Cybersecurity Data Element
  - Version 2: DRAFT National Cybersecurity Workforce Framework

For more info see: http://iac.dtic.mil/csiac/download/ia_policychart.pdf

Cybersecurity and Acquisition



Cybersecurity

2014: National Cybersecurity Protection Act
2014: Cybersecurity Workforce Assessment Act
2014: Cybersecurity Enhancement Act
2013: DoDI 5000.02 Acquisition Process (incl cyber)
2013: EO 13636: Imp Critical Infrastructure Cyber
2002: Federal Information Security Management Act
2002: Homeland Security Act (creates DHS)
2000: First documented Denial of Service attack
1995: AOL phishing (AOHell)
1988: Morris Worm appears
1986: Computer Fraud and Abuse Act
1986: Malware virus “Brain” emerged

- Agencies developing guidelines
- May involve all complexity levels (low to high)
- Relatively new and still emerging

Federal Acquisition

2015: Federal Information Technology Acquisition
Reform Act (FITARA)
2015: DoDI 5000.02 Acquisition Process
2010: DoD Better Buying Power
1996: FAA & US MINT exempt from FAR
1996: Federal Acquisition Reform Act (Clinger-Cohen)
1994: Federal Acquisition Streamlining Act (FASA)
1993-98: Defense Acquisition Reform Initiatives
1982: Special Panel on Defense Procurement
1981: Carlucci Thirty-Two Acquisition Initiatives
1979: Defense Resources Board
1962: Truth in Negotiating Act (TINA)
1947: Armed Services Procurement Act
1941: Berry Amendment
1861: Civil Sundry Appropriations Act

- Not a “one-size fits all”
- Accommodate all levels of program complexity
- Very mature and still evolving

A Cybersecurity Paradigm Shift

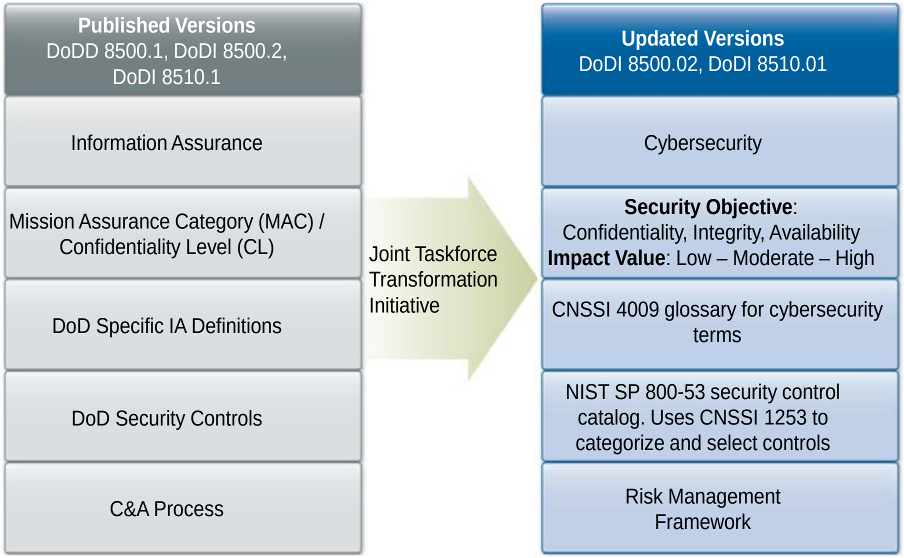
From Bolt On

- Stove-piped and bolt-on security
- Compliance & checklist mindset
- Reactive and tactical
- Point in time Certify and Accredit
- Compliance-based security
- Little or no verification of sources

To Built In

- Integrated and built-in cybersecurity
- Risk management and risk posture
- Proactive, preventive, and strategic
- Lifecycle and start early
- Technical & performance security
- Verify “trusted” products/services

Shift in orientation from a **compliance** mindset to a **risk management** mindset has driven the shift in terminology



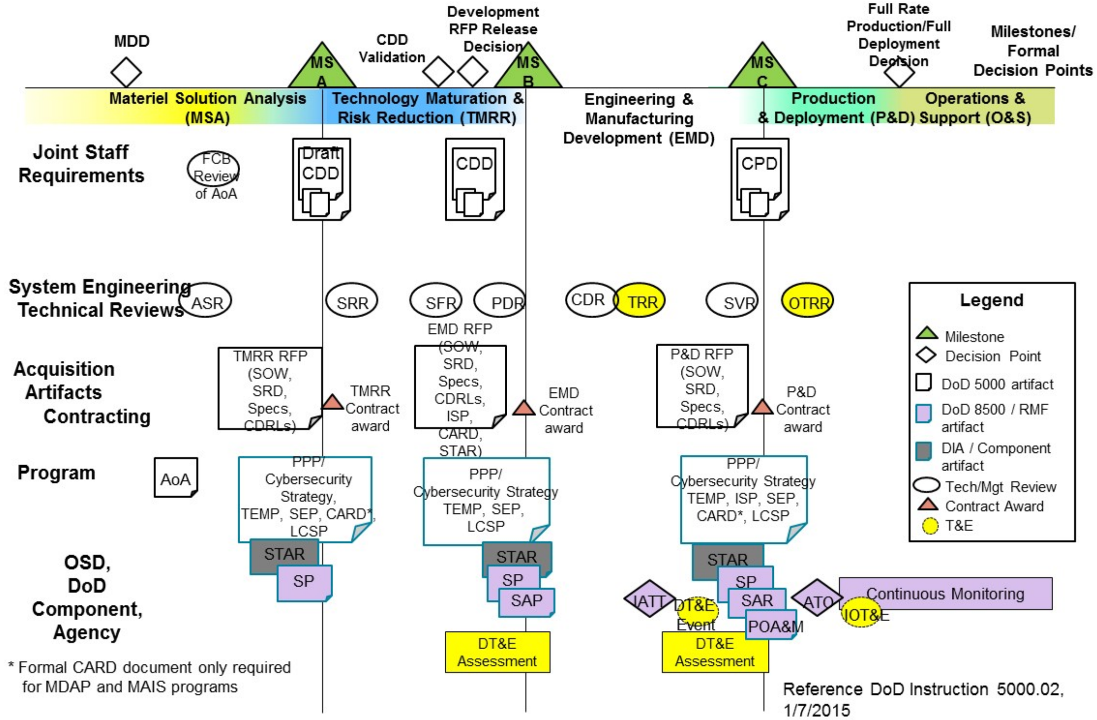
Published Versions DoDD 8500.1, DoDI 8500.2, DoDI 8510.1	**Updated Versions** DoDI 8500.02, DoDI 8510.01
Information Assurance	Cybersecurity
Mission Assurance Category (MAC) / Confidentiality Level (CL)	**Security Objective**: Confidentiality, Integrity, Availability **Impact Value**: Low – Moderate – High
DoD Specific IA Definitions	CNSSI 4009 glossary for cybersecurity terms
DoD Security Controls	NIST SP 800-53 security control catalog. Uses CNSSI 1253 to categorize and select controls
C&A Process	Risk Management Framework

Program Manager’s Challenge

> The Department must do a better job implementing Information Assurance (IA) within acquisition systems …Program Managers (PMs) frequently fail to address IA requirements early within the acquisition life cycle, and subsequently struggle during later acquisition phases to meet requirements after important design trades have been made.
>
> –Memorandum from Mrs. Katrina McFarland, Assistant Secretary of Defense (Acquisition), 11 November 2012.

IA is now called cybersecurity, adopted into the acquisition process through adoption of:

- New cybersecurity policy (DoDI 8500 and DoD 8510)
- Acquisition policy (DoDI 5000.02)


MDD
MS A
CDD Validation
Development RFP Release Decision
MS B
MS C
Full Rate Production/Full Deployment Decision
Milestones/ Formal Decision Points
Materiel Solution Analysis (MSA)
Technology Maturation & Risk Reduction (TMRR)
Engineering & Manufacturing Development (EMD)
Production & Deployment (P&D)
Operations & Support (O&S)
Joint Staff Requirements
FCB Review of AoA
Draft CDD
CDD
CPD
System Engineering Technical Reviews
ASR
SRR
SFR
PDR
CDR
TRR
SVR
OTRR
Acquisition Artifacts Contracting
TMRR RFP (SOW, SRD, Specs, CDRLs)
TMRR Contract award
EMD RFP (SOW, SRD, Specs, CDRLs, ISP, CARD, STAR)
EMD Contract award
P&D RFP (SOW, SRD, Specs, CDRLs)
P&D Contract award
Program
AoA
PPP/ Cybersecurity Strategy, TEMP, SEP, CARD*, LCSP
PPP/ Cybersecurity Strategy TEMP, SEP, LCSP
PPP/ Cybersecurity Strategy TEMP, ISP, SEP, CARD*, LCSP
OSD, DoD Component, Agency
STAR
SP
STAR
SP
SAP
DT&E Assessment
IATT
DT&E Event
STAR
SP
SAR
POA&M
DT&E Assessment
ATO
IOT&E
Continuous Monitoring
Legend
Milestone
Decision Point
DoD 5000 artifact
DoD 8500 / RMF artifact
DIA / Component artifact
Tech/Mgt Review
Contract Award
T&E

* Formal CARD document only required for MDAP and MAIS programs

Reference DoD Instruction 5000.02, 1/7/2015

Program Manager's Responsibilities

Better Buying Power 3.0

Strengthen cybersecurity throughout the product lifecycle –

The Department has initiated a series of actions to improve military system cybersecurity from concept development to disposal, but much more needs to be done. This initiative will help to focus and accelerate DoD’s efforts to address planning, designing, developing, testing, manufacturing, and sustaining activities with cyber security constantly in mind.

- **New Enclosure for DoDI 5000.02 addressing all aspects of the PM’s and other’s responsibilities for cybersecurity throughout the product lifecycle. Draft Jul 2015**

- Establish a joint analysis capability. September 2015

- Conduct an assessment of the effectiveness of the implementation of DFARS required CTI protection standards. September 2015

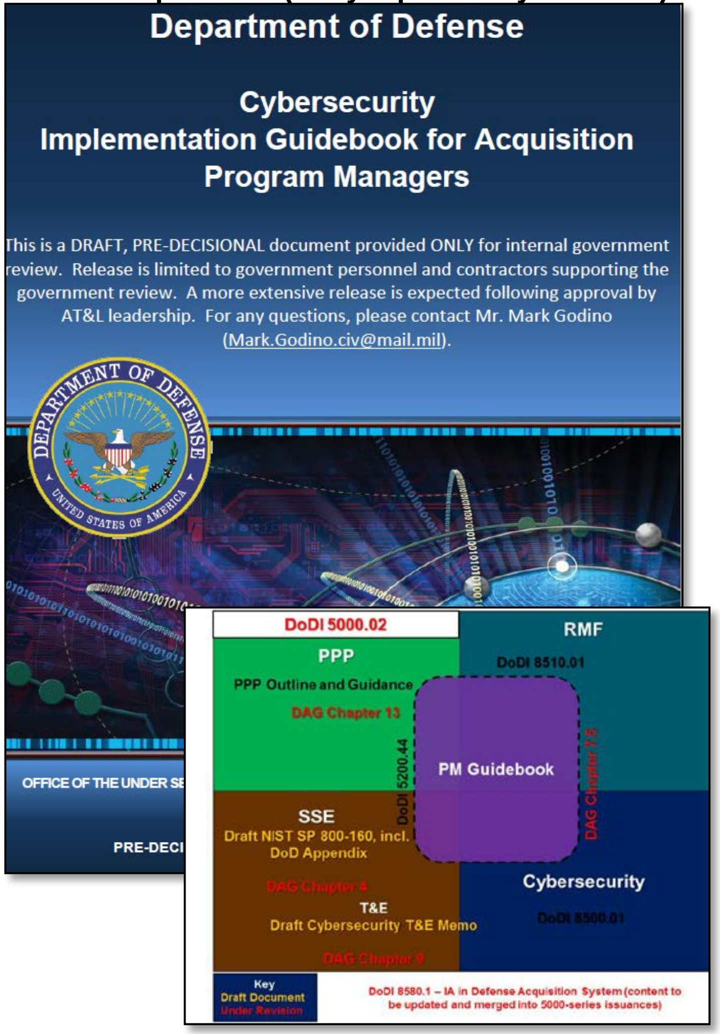
- Implement higher level protection of technical information. October 2015

- Develop education and training. December 2015

Program Manager’s Guidance

- **PMs need to integrate cybersecurity into their programs and systems**
- **Two objectives:**
  - Describe key concepts and activities for successful implementation of cybersecurity and system resilience throughout the acquisition lifecycle
  - Familiarize program managers with RMF continuous monitoring to optimize mission effects throughout the acquisition lifecycle
- **Guidebook relates content to DoD cybersecurity policy, DoD acquisition policy, and other references**

INTERNAL DRAFT VERSION 0.9971
April 2015 (not yet publically released)



Department of Defense

Cybersecurity
Implementation Guidebook for Acquisition
Program Managers

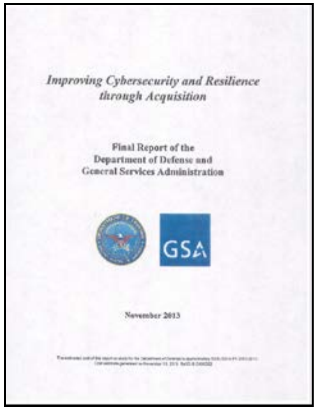
This is a DRAFT, PRE-DECISIONAL document provided ONLY for internal government review. Release is limited to government personnel and contractors supporting the government review. A more extensive release is expected following approval by AT&L leadership. For any questions, please contact Mr. Mark Godino (Mark.Godino.civ@mail.mil).

OFFICE OF THE UNDER SE

PRE-DECI

Program Manager’s Accountability

- **Report focus:**
  - Incorporating cybersecurity into technical requirements
  - Developing consistency in interpretation and application of procurement rules
  - Ensuring Government accountability for cyber risk management throughout the acquisition lifecycle



Improving Cybersecurity and Resilience through Acquisition

Final Report of the
Department of Defense and
General Services Administration

November 2013

Report Recommendations	Working Group Lead
I. Institute **baseline security requirements** as a condition for award	Don Davidson, OSD
II. Address cybersecurity in relevant **training**	Andre Wilkinson, DHS
III. Develop common **cybersecurity definitions** for federal acquisitions	Jon Boyens, NIST
IV. Institute a Federal acquisition cyber **risk management strategy**	Don Johnson, OSD
V. Include requirement to purchase from OEM, authorized resellers, or other **trusted sources**	Emile Monette, GSA
VI. Increase **Government accountability** for cyber risk management	Joe Jarzombek, DHS

Source: DoD and GSA Report on “Improving Cybersecurity and Resilience through Acquisition”

Report Recommendation VI

Recommendation	Description and Highlights
VI. **Increase Government Accountability for Cyber Risk Management** ***Key acquisition recommendation** **--Critical for PMs to understand cybersecurity requirements development and source selection**	A. Identify and modify acquisition practices that contribute to cyber risk B. Integrate security standards into acquisition planning and contract administration C. Incorporate cyber risk into enterprise risk management and ensure key decision makers (e.g., Program Executive) are accountable: 1. Address cyber risk when defining requirement and analyzing solution 2. Ensure and certify cybersecurity requirements are adequately reflected in the solicitation 3. Participate in evaluation and ensure best value proposal meets the solicitation cybersecurity requirements 4. Certify contract performance reviews of cybersecurity (e.g., conformance testing, regression testing, technology refresh, supply chain management, engineering change proposals, etc…) are conducted in accordance with prescribed standards*

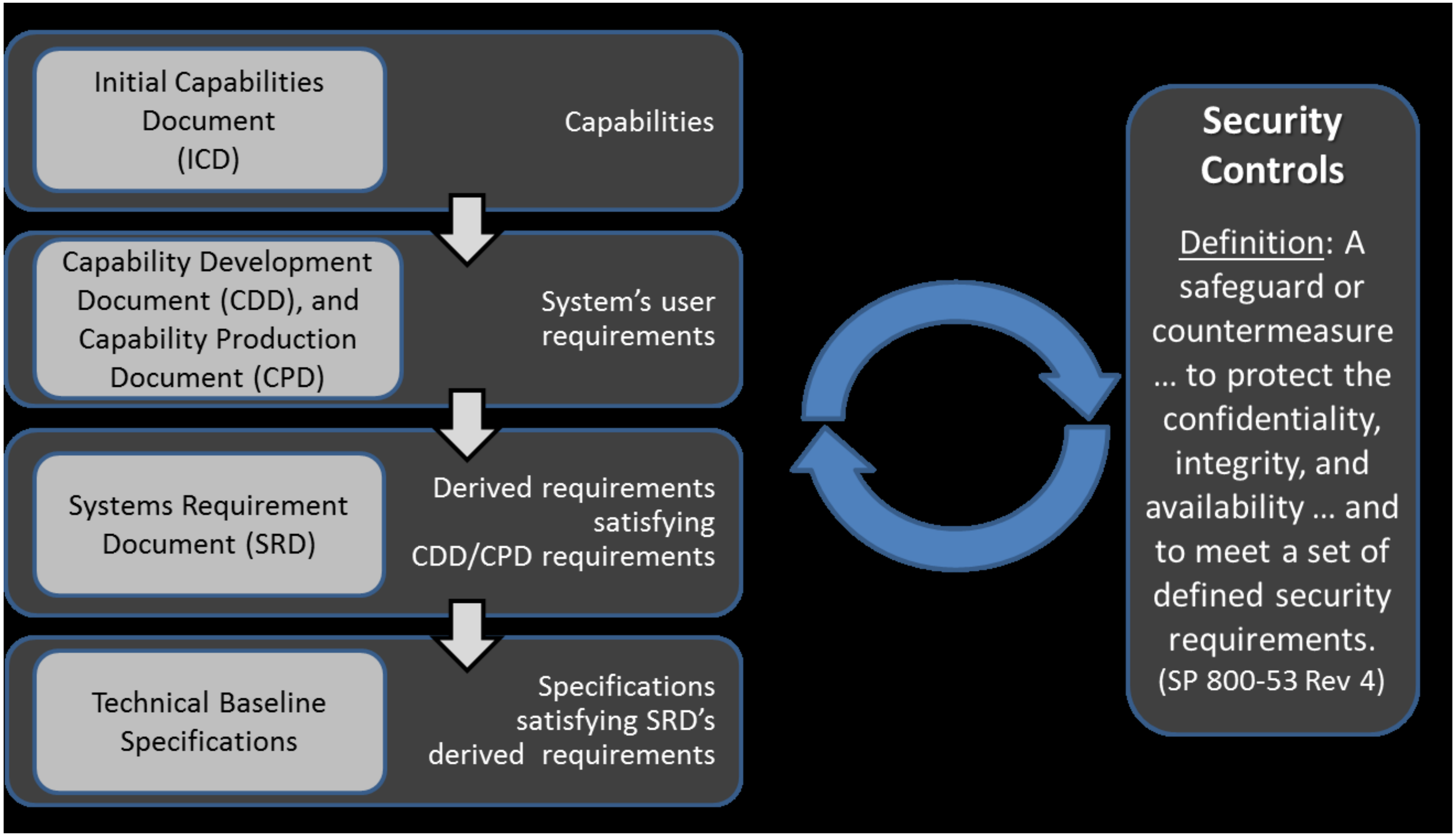
Source: DoD and GSA Report on "Improving Cybersecurity and Resilience through Acquisition"

Acquisition Life Cycle

- **Acquisition Planning**
  - Conduct Market Research and Request for Information
  - Develop Acquisition Plan
  - Develop Cybersecurity Requirements documents
    - **SOW, PWS, SOO, Specification**
    - References and applicable documents
- Solicitation Development
  - **Request for Proposal (RFP)**
  - Develop Contract Data Requirements List (CDRL)
  - Identify clauses and special restrictions (I and H)
  - **Instructions and Evaluation Criteria (L and M)**
- **Source Selection**
- **Award and Post-Award Management**

SOW/RFP/L&M are critical documents to integrate cybersecurity into the acquisition process

Cybersecurity Requirements Development


Initial Capabilities Document (ICD)
Capabilities
Capability Development Document (CDD), and Capability Production Document (CPD)
System's user requirements
Systems Requirement Document (SRD)
Derived requirements satisfying CDD/CPD requirements
Technical Baseline Specifications
Specifications satisfying SRD's derived requirements
Security Controls

Definition: A safeguard or countermeasure … to protect the confidentiality, integrity, and availability … and to meet a set of defined security requirements. (SP 800-53 Rev 4)

Source: DoD Cybersecurity Implementation Guidebook for Acquisition Program Managers

Relationship between requirements, specifications, and security controls

Statement of Work (SOW) Outline

Weave Cybersecurity Content Throughout the SOW/PWS/SOO

- **Section 1: Scope**
  - Section 1.1: Introduction
  - Section 1.2: Background
  - Section 1.3: Scope
- **Section 2: Applicable Documents**
  - Section 2.1: Department or Agency specific Specifications
  - Section 2.2: Department or Agency specific Standards
  - Section 2.3: Other Relevant Documents or Publications
- **Section 3: Requirements**
  - Section 3.1: General Requirements
  - Section 3.2: Technical Objectives and Goals
  - Section 3.3: Specific Requirements
- **Section 4: Contract Deliverables**
- **Section 5: Security**
- **Section 6: Personnel**

Primary Source: DoD MIL HDBK 254D: DoD Handbook for Preparation of Statement of Work (SOW)

Solicitation (RFP) Content

- **A – Solicitation/contract form -** None anticipated
- **B – Supplies or services and prices/costs**
  - Review Contract Data Requirements List (CDRL) cybersecurity reports
  - Consider cost recovery mechanisms (CLIN structure, SLAs, incentives)
- **C – Description/Specifications/Statement of Work**
  - Clearly define performance-based outcomes directly tied to program objectives, stakeholder cybersecurity requirements
  - Specify the CNSSI No. 1253 categorization of the item to be acquired
- **D – Packaging and marking -** None anticipated
- **E – Inspection and acceptance**
  - Develop cybersecurity quality assurance surveillance plan (DoD)
- **F – Deliveries or performance**
  - Ensure cybersecurity-related items are addressed
- **G – Contract administration data -** None anticipated
- **H – Special contract requirements**
  - Cybersecurity-specific contract clauses (e.g., reporting or disclosure)

Source: DoD Cybersecurity Implementation Guidebook for Acquisition Program Managers

Solicitation (RFP) Content

- **I – Contract clauses**
  - Cybersecurity-specific contract clauses
  - Cybersecurity Key Personnel (some agencies include with Section H)
- **J – List of Attachments**
  - Applicable attachments related to cybersecurity
- **K – Representations, Certifications, Statements of Offerors**
  - Include requests for certifications that support the cybersecurity strategy (NSA certifications of cryptographic algorithms or equipment, and certification of cross-domain solutions)
- **L and M – Proposal Information and Evaluation Criteria**
  - Ensure evaluation factors and standards differentiate proposals
  - Define measures to evaluate qualification of cybersecurity staff
  - Include critical cybersecurity program objectives in evaluation factors

Source: DoD Cybersecurity Implementation Guidebook for Acquisition Program Managers

Cybersecurity Evaluation Criteria (Section M)

Notional or suggested factors and sub-factors

Development

- Approach to certifying (8570, NICE, other) developers and ensuring continued certifications
- Approach to integrating SSE into the lifecycle (e.g., development, test)
- Approach to evaluating, documenting and managing risk (e.g., RMF)
- Degree to which tools reflect best practices in selection and application (what tools are used and when)
- SSE Approach to ensure Mission Assurance, Resilience

Systems

- Demonstrated ability to detect and prevent attacks
- Approach to detecting and minimizing data exfiltration and data loss
- Approach to integrating and enhancing operational tools
- Approach to testing and validating initial and continued competency of staff
- Degree to which operational approach integrates with current or planned CONOPS, BCP, information architecture, programs or initiatives

How Would You Prioritize These?

Cybersecurity Evaluation Criteria (Section M)

Notional or suggested factors and sub-factors

Hardware/Software

- Degree to which trusted sources are used and provenance of supplied components is maintained
- Approach to restricting physical access of non-authorized personnel
- Use of trusted foundries for critical hardware and software components
- Sparing approach
- Approach to detecting counterfeit components
- Degree to which supply chain diversity is implemented

Services

- Approach to developing software case studies for assurance, resilience
- Approach to ensuring trustworthiness of key personnel
- Approach to conducting assessments
- Degree to which cybersecurity is included in design trades
- Degree to which provided components is non-attributable to acquiring agency
- Testing approach to ensure supplied components (hardware & software) meet specifications

How Would You Prioritize These?

Systems Security Engineering Criteria

- Consider who designs, develops, and implements an integrated end-to-end security architecture (who is the integrator)
- Identify the relationships of security artifacts, analysis, processes, and deliverables to overall program activities (e.g., security analyses at major reviews)
- Require security readiness assessments and deliverables at each major milestone
- Include applicable agency mandates, polices or instructions as compliance documents

Include security engineering requirements and policy mandates in the solicitation

Summary

- Cyber breaches and threats are real and increasing
- Government cybersecurity policies and guidance have increased in last few years
- Government is shifting from compliance-based requirements to cybersecurity risk-based management framework
- Cybersecurity needs to be integrated into program acquisition and execution support to facilitate program management success
- Full research paper with content and references will be available publicly July/August 2015 timeframe through www.mitre.org