# Technology and Program Protection

Ms. Melinda Reed
Director, Resilient Systems (RS)

OUSD(R&E)

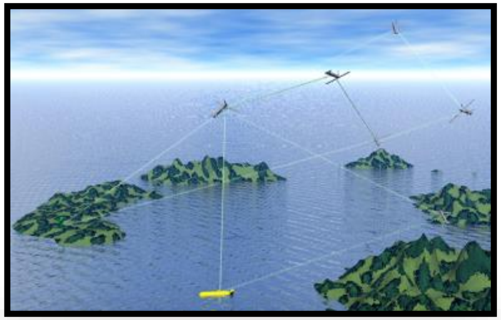
NDIA Systems Engineering Division
Annual Meeting
December 5, 2019

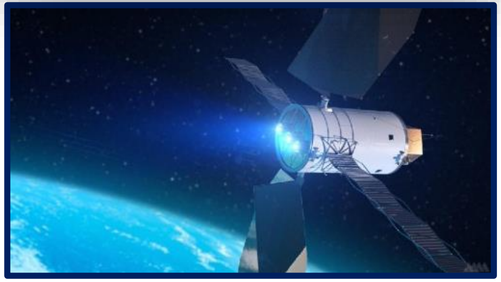
*https://www.CTO.mil* *@DoDCTO*

Distribution Statement A: Approved for public release. Distribution is unlimited.

# Under Secretary of Defense for Research and Engineering Mission

- Ensure Technological Superiority for the U.S. Military
  - Set the technical direction for the Department of Defense
  - Champion and pursue new capabilities, concepts, and prototyping activities throughout the DoD research and development enterprise
- Bolster Modernization
  - Pilot new acquisition pathways and concepts of operation
  - Accelerate capabilities to the warfighter





Distribution Statement A: Approved for public release. Distribution is unlimited.

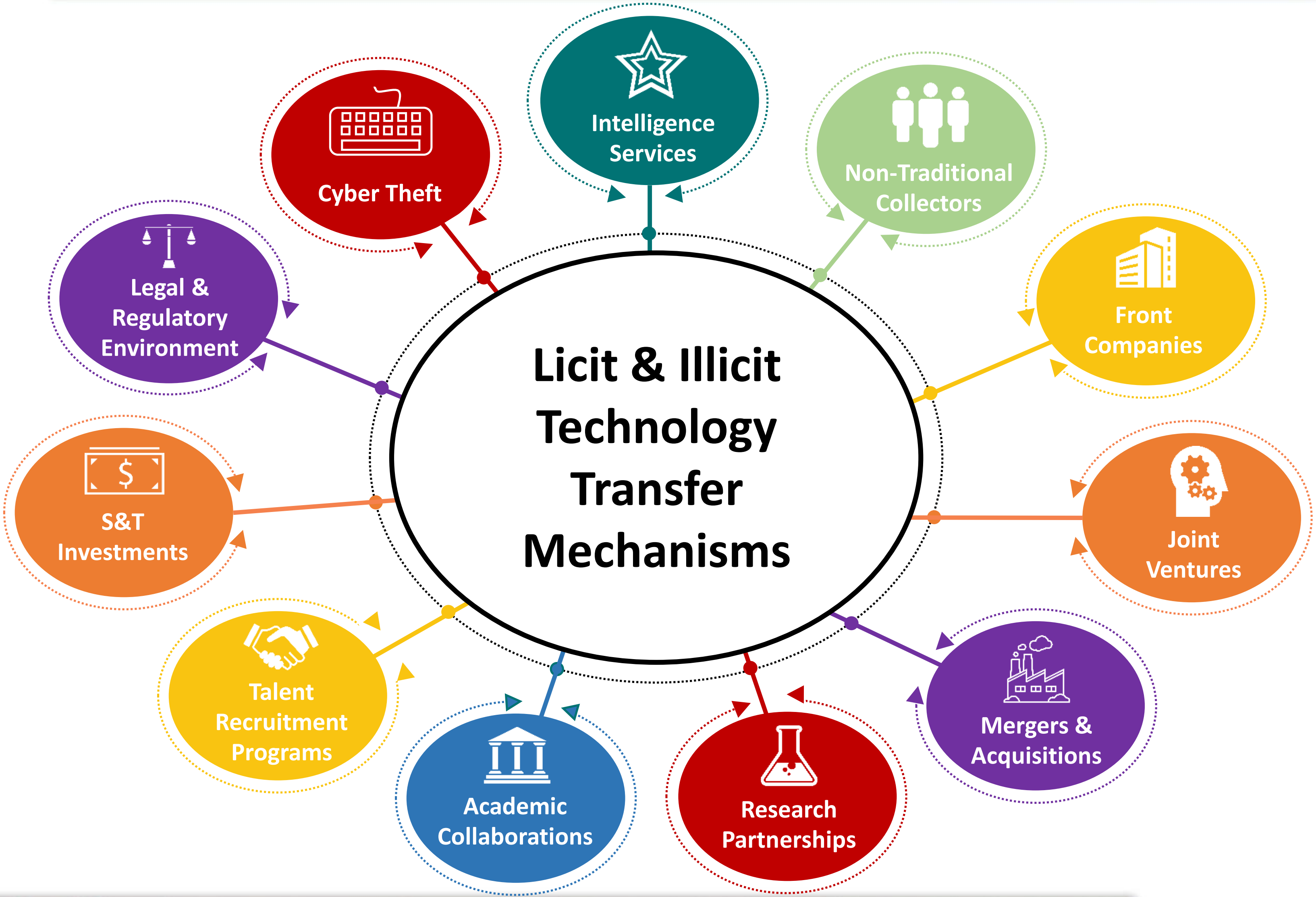
# Modernization Priorities

> ***“We cannot expect success fighting tomorrow’s conflicts with yesterday’s weapons or equipment.”***
>
> **– National Defense Strategy**

- 5G Network Technology
- Autonomy
- Biotechnology
- Cyber
- Directed Energy
- Fully Networked Command, Control, and Communications
- Hypersonics
- Machine Learning / Artificial Intelligence
- Microelectronics
- Quantum Science
- Space

***There is a Portfolio Manager (Assistant Director) who is responsible for establishing the DoD-wide, mission-focused strategy and execution plan for each modernization priority.***

# Threats to U.S. National & Economic Security



Licit & Illicit Technology Transfer Mechanisms

Intelligence Services

Non-Traditional Collectors

Front Companies

Joint Ventures

Mergers & Acquisitions

Research Partnerships

Academic Collaborations

Talent Recruitment Programs

S&T Investments

Legal & Regulatory Environment

Cyber Theft

Distribution Statement A: Approved for public release. Distribution is unlimited.

# Maintaining Technology Advantage

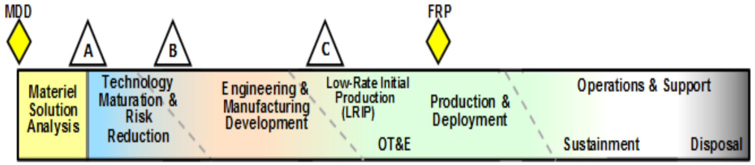
- Technology advantage stems from multiple elements:
  - People, Technology, Innovation, Supply Chain, Fabrication, Application
- Technology protection approach:
  - Prioritize what to protect
  - Apply appropriate protections through the life cycle
  - Protect unique aspects of advantage (e.g., specialized manufacturing methods)
- Success is gained through rapid integration and delivery of advanced, resilient capabilities

**We Must Create As Well As Protect Our National and Economic Security.**

# Ensuring Cyber Resilient Systems

- ***Threat:***
  - Adversary who seeks to exploit vulnerabilities to:
    - Acquire program and system information;
    - Disrupt or degrade system performance;
    - Obtain or alter U.S. warfighting capability
- ***Vulnerabilities:***
  - Found in programs, organizations, personnel, networks, systems, and supporting systems
  - Inherent weaknesses in hardware and software can be used for malicious purposes
  - Weaknesses in processes can be used to intentionally insert malicious hardware and software
  - Unclassified design information within the supply chain can be aggregated
  - U.S. warfighting capability that provides a technological advantage can be lost or sold
- ***Consequences:***
  - Loss of technological advantage
  - System impact – corruption and disruption
  - Mission impact – capability is countered or compromises mission success

***Access points are throughout the acquisition life cycle…***

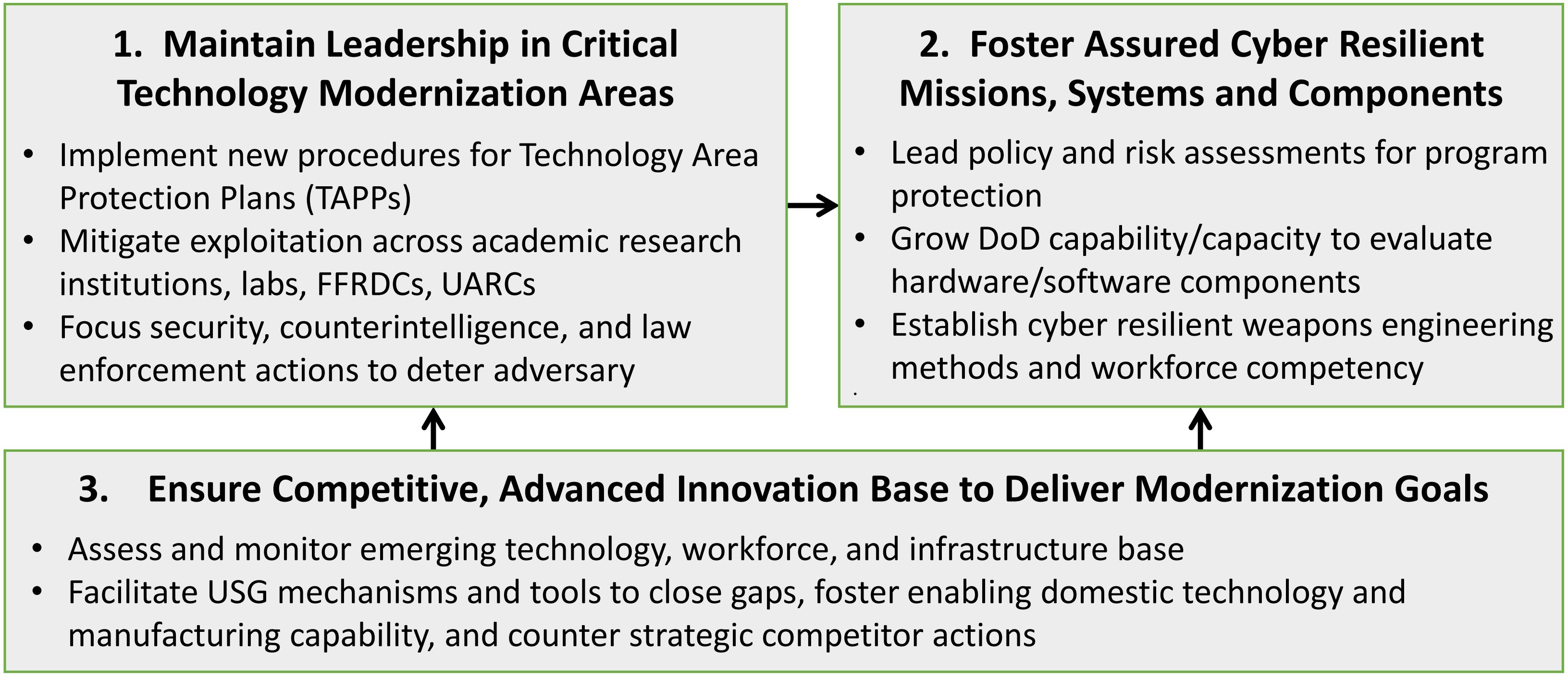

MDD
A
B
C
FRP
Materiel Solution Analysis
Technology Maturation & Risk Reduction
Engineering & Manufacturing Development
Low-Rate Initial Production (LRIP)
OT&E
Production & Deployment
Operations & Support
Sustainment
Disposal

***…and across numerous supply chain entry points***

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

# STP&E: Vision and Key Outcomes

VISION: Enduring warfighter and technology dominance enabled through superior mission systems resilient to exploitation; a competitive, assured national security innovation base; and preservation of advanced technologies and practices



### 1. Maintain Leadership in Critical Technology Modernization Areas

- Implement new procedures for Technology Area Protection Plans (TAPPs)
- Mitigate exploitation across academic research institutions, labs, FFRDCs, UARCs
- Focus security, counterintelligence, and law enforcement actions to deter adversary

### 2. Foster Assured Cyber Resilient Missions, Systems and Components

- Lead policy and risk assessments for program protection
- Grow DoD capability/capacity to evaluate hardware/software components
- Establish cyber resilient weapons engineering methods and workforce competency

### 3. Ensure Competitive, Advanced Innovation Base to Deliver Modernization Goals

- Assess and monitor emerging technology, workforce, and infrastructure base
- Facilitate USG mechanisms and tools to close gaps, foster enabling domestic technology and manufacturing capability, and counter strategic competitor actions

***STP&E provides leadership focal point and focus for comprehensive Promote-Protect-Counter campaign***

# Program Protection Planning to Improve Cyber Resiliency

## Program Protection & Cybersecurity

## Policies and Programs

### Technology

**Key Protection Activities:**

- Anti-Tamper
- Defense Exportability Features
- CPI Protection List
- Acquisition Security Database

**Goal**: Prevent the compromise or loss of critical technologies

### Components

**Key Protection Activities:**

- Software Assurance
- Hardware Assurance/Trusted Foundry
- Supply Chain Risk Management
- Anti-counterfeits
- Joint Federated Assurance Center (JFAC)

**Goal**: Protect critical system components (hardware, software) from malicious exploitation

### Information

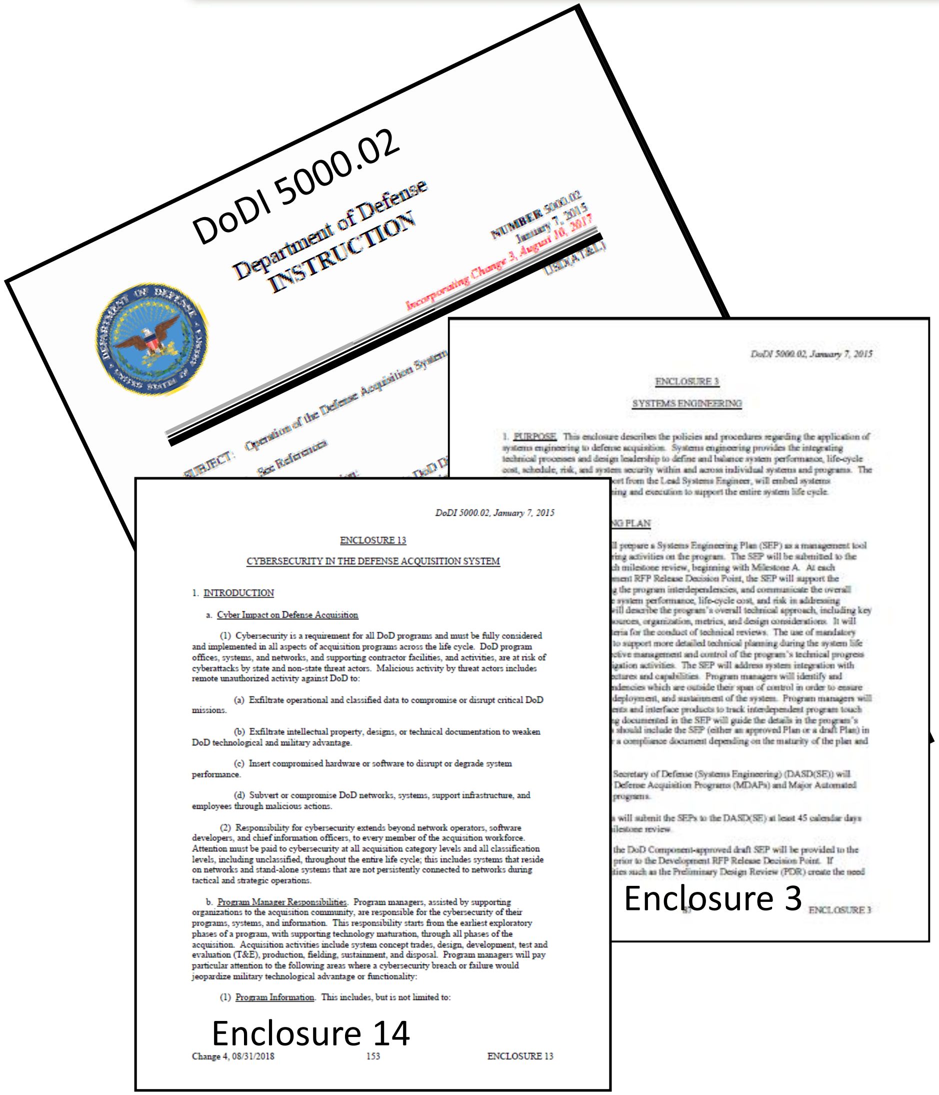
**Key Protection Activities:**

- Classification
- Export Controls
- Information Security
- Joint Acquisition Protection & Exploitation Cell (JAPEC)

**Goal**: Ensure critical system and program data is protected from adversary collection

***Protecting Warfighting Capability Throughout the Lifecycle***

# Current Program Protection Planning in DoDI 5000.02 Acquisition Policy



DoDI 5000.02

Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015
Incorporating Change 3, August 10, 2017
USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

See References

DoD Di

DoDI 5000.02, January 7, 2015

ENCLOSURE 3

SYSTEMS ENGINEERING

1. PURPOSE. This enclosure describes the policies and procedures regarding the application of systems engineering to defense acquisition. Systems engineering provides the integrating technical processes and design leadership to define and balance system performance, life-cycle cost, schedule, risk, and system security within and across individual systems and programs. The
…ort from the Lead Systems Engineer, will embed systems
…ing and execution to support the entire system life cycle.

…NG PLAN

…ll prepare a Systems Engineering Plan (SEP) as a management tool
…ring activities on the program. The SEP will be submitted to the
…ch milestone review, beginning with Milestone A. At each
…ment RFP Release Decision Point, the SEP will support the
…g the program interdependencies, and communicate the overall
…e system performance, life-cycle cost, and risk in addressing
…will describe the program's overall technical approach, including key
…sources, organization, metrics, and design considerations. It will
…teria for the conduct of technical reviews. The use of mandatory
…to support more detailed technical planning during the system life
…ctive management and control of the program's technical progress
…igation activities. The SEP will address system integration with
…ctures and capabilities. Program managers will identify and
…ndencies which are outside their span of control in order to ensure
…deployment, and sustainment of the system. Program managers will
…ents and interface products to track interdependent program touch
…g documented in the SEP will guide the details in the program's
…should include the SEP (either an approved Plan or a draft Plan) in
…r a compliance document depending on the maturity of the plan and

…Secretary of Defense (Systems Engineering) (DASD(SE)) will
…Defense Acquisition Programs (MDAPs) and Major Automated
…programs.

…will submit the SEPs to the DASD(SE) at least 45 calendar days
…ilestone review.

…the DoD Component-approved draft SEP will be provided to the
…prior to the Development RFP Release Decision Point. If
…ties such as the Preliminary Design Review (PDR) create the need

Enclosure 3

ENCLOSURE 3

DoDI 5000.02, January 7, 2015

ENCLOSURE 13

CYBERSECURITY IN THE DEFENSE ACQUISITION SYSTEM

1. INTRODUCTION

a. Cyber Impact on Defense Acquisition

(1) Cybersecurity is a requirement for all DoD programs and must be fully considered and implemented in all aspects of acquisition programs across the life cycle. DoD program offices, systems, and networks, and supporting contractor facilities, and activities, are at risk of cyberattacks by state and non-state threat actors. Malicious activity by threat actors includes remote unauthorized activity against DoD to:

(a) Exfiltrate operational and classified data to compromise or disrupt critical DoD missions.

(b) Exfiltrate intellectual property, designs, or technical documentation to weaken DoD technological and military advantage.

(c) Insert compromised hardware or software to disrupt or degrade system performance.

(d) Subvert or compromise DoD networks, systems, support infrastructure, and employees through malicious actions.

(2) Responsibility for cybersecurity extends beyond network operators, software developers, and chief information officers, to every member of the acquisition workforce. Attention must be paid to cybersecurity at all acquisition category levels and all classification levels, including unclassified, throughout the entire life cycle; this includes systems that reside on networks and stand-alone systems that are not persistently connected to networks during tactical and strategic operations.

b. Program Manager Responsibilities. Program managers, assisted by supporting organizations to the acquisition community, are responsible for the cybersecurity of their programs, systems, and information. This responsibility starts from the earliest exploratory phases of a program, with supporting technology maturation, through all phases of the acquisition. Acquisition activities include system concept trades, design, development, test and evaluation (T&E), production, fielding, sustainment, and disposal. Program managers will pay particular attention to the following areas where a cybersecurity breach or failure would jeopardize military technological advantage or functionality:

(1) Program Information. This includes, but is not limited to:

Enclosure 14

Change 4, 08/31/2018 153 ENCLOSURE 13

- Enclosure 3, *System Engineering*
  - Employ System Security Engineering and develop a Program Protection Plan (PPP) to manage program protection risks to DoD warfighting capability
  - Use countermeasures to mitigate risks: anti tamper, supply chain risk management (SCRM), hardware assurance, software assurance, and cybersecurity practices, where appropriate
- Enclosure 14, *Cybersecurity in the Defense Acquisition System*
  - Establishes and assigns Program Manager responsibilities for Cybersecurity, utilizing Program Protection Planning

Distribution Statement A: Approved for public release. Distribution is unlimited.

# Technology and Program Protection → New DoD Instruction

- Maintain program protection policy from DoDI 5000.02 Enclosure 3 and 14 (Cybersecurity in the Defense Acquisition, and Systems Engineering)
- Introduce Technology Area Protection Plans (TAPP)
- Establish responsibilities and procedures for Chief Technologists and Engineers to cost effectively employ risk-based protections of technology and programs
- Aligns program protections with Acquisition Pathways

**Supports the revised DoD Instruction 5000.02, Operation of the Adaptive Acquisition Framework**

# TAPP Background

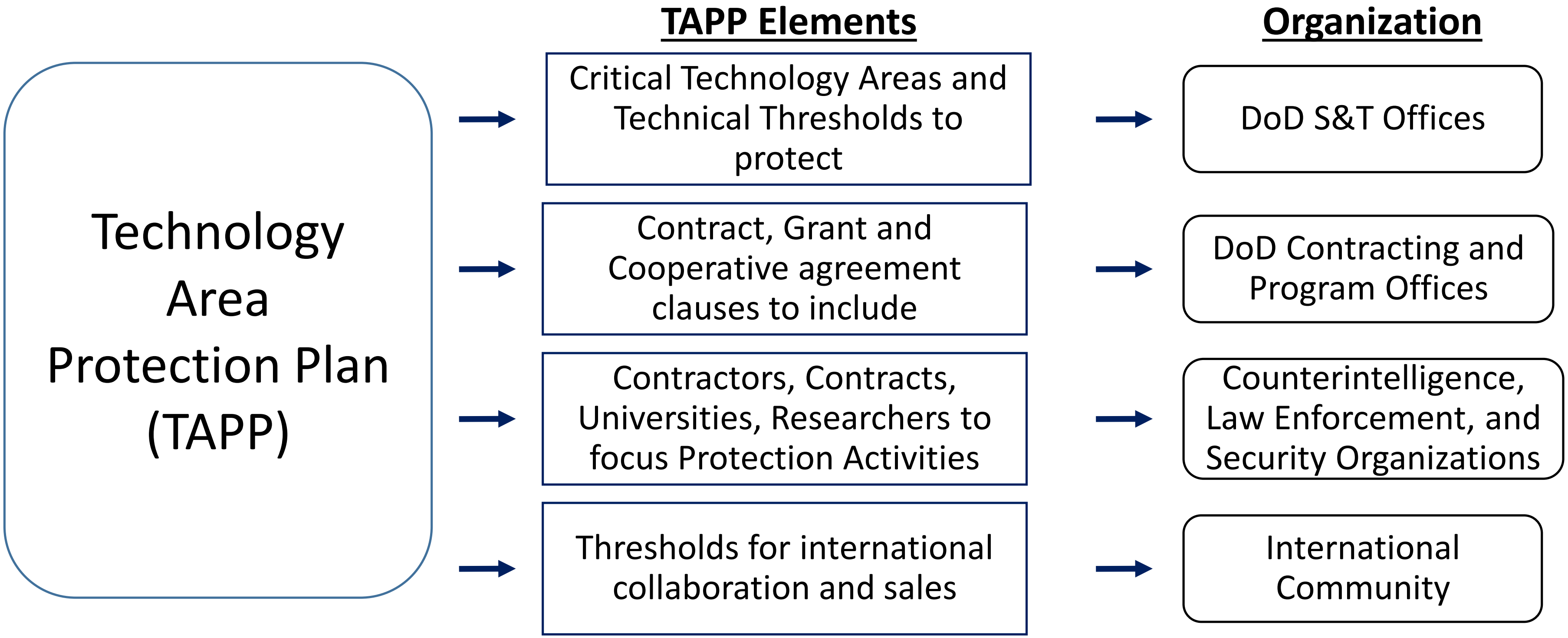
- The current threat environment necessitates a coordinated approach to protecting technologies and their engineering/integration
- Program Protection Plans (PPP) exist, but only for programs Post-Milestone A
- Technology protection should be enterprise-wide with close collaboration from the research community (DoD Labs, FFRDCs/UARCs, Universities)

- Interagency and International partnerships are critical for horizontal protection
- Security, Counterintelligence, and Intelligence activities will play a key support role in identifying and mitigating threats to technologies that may have long-lasting effects on the U.S. military advantage

FFRDC - Federally Funded R&D Center
UARC - University Affiliated Research Center

# What Information is in a TAPP and Who Uses It?

Technology identified for protection is provided to stakeholders – both S&T entities and protection entities – to support protection efforts and create an awareness of newly identified technologies, threats, and if needed the reprioritization of protection efforts



Technology Area Protection Plan (TAPP)

**TAPP Elements**

- Critical Technology Areas and Technical Thresholds to protect
- Contract, Grant and Cooperative agreement clauses to include
- Contractors, Contracts, Universities, Researchers to focus Protection Activities
- Thresholds for international collaboration and sales

**Organization**

- DoD S&T Offices
- DoD Contracting and Program Offices
- Counterintelligence, Law Enforcement, and Security Organizations
- International Community

**Data from the TAPP informs all of Government protection effort for critical DoD technologies**

# Balancing Protection and Promotion of U.S. Technology and Innovation Base

- We protect to retain U.S. advantage in current and emergent technologies and the industrial innovation base developing, manufacturing, and sustaining them
- We promote to ensure a long-term viable technology development and innovation base in support of modernization priorities

### *Protect Goals*

- Mitigate espionage and cyber attacks
- Sustain economic prosperity and protect critical assets from foreign ownership
- Deny access to critical technology, know-how, infrastructure and information
- Avoid technology transfer and proliferation
- Prevent reverse engineering to exploit U.S. technology
- Secure personally identifiable information
- Reduce foreign competitor dependency

### *Promote Goals*

- Reduce entry barriers and promote rapid adoption
- Maintain startup health
- Incentivize and support industry’s investments in infrastructure, workforce development, and machinery to increase capacity
- Improve manufacturing materials and processes
- Sustain defense unique suppliers

- It is our responsibility to create a balance that allow us to protect our critical technology while sustaining our industrial base ability to innovate and compete in the global markets.

# Focusing Programs/Tools to Protect and Promote U.S. Technology and Innovation Base

## Protect - Promote

| | | | |
|---|---|---|---|
| Technology Area Protection Plans (TAPPs) | Defense Production Act Title III | Manufacturing Technology (ManTech) | STEM Programs |
| Export Controls | Manufacturing Innovation Institutes | Small Business Innovation Research | Small Business Technology Transfer |
| Hart-Scott-Rodino Act | Industrial Base Analysis & Sustainment | Warstopper Program | International Cooperation Programs |
| Committee on Foreign Investments in U.S. | Policies and Regulations | Acquisition Programs | Other U.S. Government Programs |

# DoD Research and Engineering Enterprise

## ***Creating the Technologies of the Future Fight***

| DoD Research and Engineering Enterprise | Twitter |
|---|---|
| *https://www.CTO.mil* | *@DoDCTO* |