DSB Task Force on

CYBER SUPPLY CHAIN

Overall Marking is Distribution A

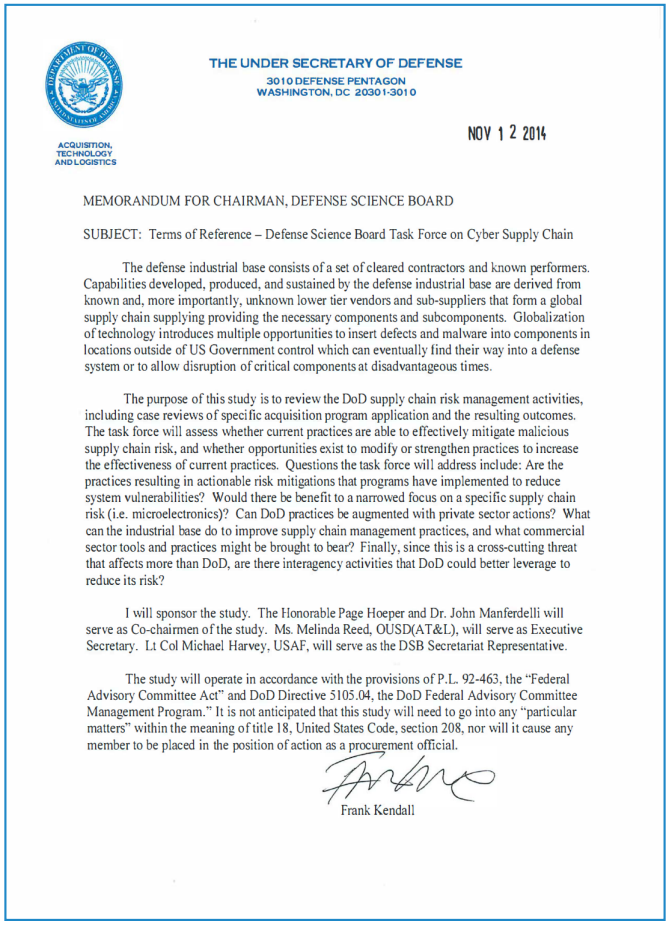
Distribution A: Approved for public release; distribution is unlimited.

Executive Briefing
July 2017

Study Objectives and Scope

What we studied:

- Supply chain that provides microelectronic hardware and embedded software in weapons systems across weapons lifetime
  - Includes high-level logic chips such as application specific integrated circuits (ASICs) and field-programmable gate arrays (FPGAs)
  - Also includes much lower-level electronics such as supplies and batteries, many of which contain “micro code”
- Current practices to identify, protect, detect, respond to, and recover from supply chain attacks involving malicious insertions and exploitation of latent vulnerabilities
- Strategies and technologies to make it harder for attackers to succeed and to limit the impact of a successful attack



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

ACQUISITION, TECHNOLOGY AND LOGISTICS

NOV 1 2 2014

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Cyber Supply Chain

The defense industrial base consists of a set of cleared contractors and known performers. Capabilities developed, produced, and sustained by the defense industrial base are derived from known and, more importantly, unknown lower tier vendors and sub-suppliers that form a global supply chain supplying providing the necessary components and subcomponents. Globalization of technology introduces multiple opportunities to insert defects and malware into components in locations outside of US Government control which can eventually find their way into a defense system or to allow disruption of critical components at disadvantageous times.

The purpose of this study is to review the DoD supply chain risk management activities, including case reviews of specific acquisition program application and the resulting outcomes. The task force will assess whether current practices are able to effectively mitigate malicious supply chain risk, and whether opportunities exist to modify or strengthen practices to increase the effectiveness of current practices. Questions the task force will address include: Are the practices resulting in actionable risk mitigations that programs have implemented to reduce system vulnerabilities? Would there be benefit to a narrowed focus on a specific supply chain risk (i.e. microelectronics)? Can DoD practices be augmented with private sector actions? What can the industrial base do to improve supply chain management practices, and what commercial sector tools and practices might be brought to bear? Finally, since this is a cross-cutting threat that affects more than DoD, are there interagency activities that DoD could better leverage to reduce its risk?

I will sponsor the study. The Honorable Page Hoeper and Dr. John Manferdelli will serve as Co-chairmen of the study. Ms. Melinda Reed, OUSD(AT&L), will serve as Executive Secretary. Lt Col Michael Harvey, USAF, will serve as the DSB Secretariat Representative.

The study will operate in accordance with the provisions of P.L. 92-463, the “Federal Advisory Committee Act” and DoD Directive 5105.04, the DoD Federal Advisory Committee Management Program.” It is not anticipated that this study will need to go into any “particular matters” within the meaning of title 18, United States Code, section 208, nor will it cause any member to be placed in the position of action as a procurement official.

Frank Kendall

Problem Context

- Assuring the integrity of weapons systems supply chain has become more difficult and requires ever increasing vigilance and sophistication in acquisition and sustainment; factors include:
  - Increased globalization and decreased control over suppliers – particularly commercial-off-the-shelf (COTS) suppliers
    - Parts information asymmetry
    - Reduced technical exclusivity
  - Increased complexity – most electronics contain programmable components
    - 5590 battery: primary battery used in tactical communications in many DoD systems
    - BIOS: has increased complexity by a factor of more than a million between 1999 and 2012
  - Well-designed and well-manufactured complex systems can have latent vulnerabilities
  - Subsequent system modification, even some intended to fix vulnerabilities, have potential to expand attack surfaces
  - Importance of intelligent systems – essential to Third Offset
- Supply chain integrity encompasses COTS hardware and software, systems developed by DoD Program Offices, and sustainment of fielded systems

These factors preclude "simple" chain integrity measures like maintaining exclusive control over all suppliers, exhaustive delivery based testing, or substantially reducing the complexity or capabilities of weapons systems

Current Practices as chartered

- **Government-Industry Data Exchange Program (GIDEP)**
  - A voluntary activity between government and industry participants reporting component information to a shared database seeking to reduce or eliminate expenditures of resources by sharing technical information
    - Begun in 1959 as IDEP; became GIDEP in 1973
    - Defense Standardization Program Office (DLA) is program manager
- **DoD Program Protection Plans (PPPs)**
  - A PPP is a single source document used to coordinate and integrate all protection efforts for an major defense acquisition program
  - The integrating process for managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability, or supply chain exploit/insertion, and battlefield loss throughout the acquisition lifecycle

National Defence / Défense nationale

Current Practices as chartered

Congress, through NDAA 2014 Section 937, 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"

JFAC: Joint Federated Assurance Center

- Develops, maintains, and offers software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the Military Departments, Defense Agencies and other DoD organizations (established February, 2015)

JAPEC: Joint Acquisition Protection and Exploitation Cell

- Integrates and coordinates analysis to enable Controlled Technology Information (CTI) protection efforts across the DoD enterprise to proactively mitigate future losses, and exploit opportunities to deter, deny, and disrupt adversaries that may threaten US military advantage

Summary of findings

- DoD cyber supply chains are unavoidably dependent on commercial, globally produced microelectronics and embedded software
- DoD weapons systems are at risk from:
  - Exploitation of latent vulnerabilities
  - Malicious insertions by sophisticated adversaries
- Current program protection practices are inadequate:
  - Lack clear guidance and expert support for acquisition office personnel
  - Lack continuity through program life-cycles
  - Lack clear guidance and expert support for operations sustainment and personnel – to prevent, detect and recover from exploited supply chain vulnerabilities
- Weapons in the field today lack PPPs and disciplined program protection practices
- Technologies to mitigate vulnerabilities are immature
  - Improving resilience and diversity of system designs
  - Pedigree and provenance tracking, anti-tamper technologies, trusted foundry alternatives, etc.

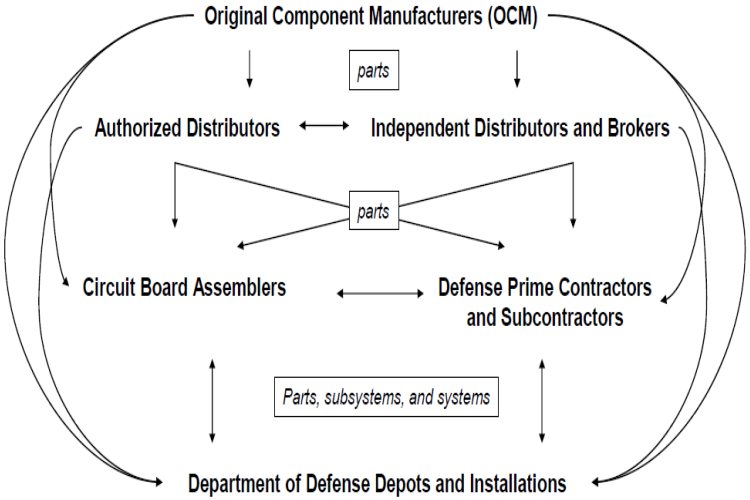
Recent Cyber Awakening demonstrations highlight the potential for real operational consequences

Three Distinct Supply Chains Present Broad Attack Surface

Multiple industry sectors feed 3 DoD Supply Chains

Each sector sells to the others

None of the three can be assured to the lowest tier supplier



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*, November 2009.

1. Global commercial supply chain
   - Easiest target for malicious insertion
   - Hardest target for precise & impactful effects
   - Feeds other supply chains

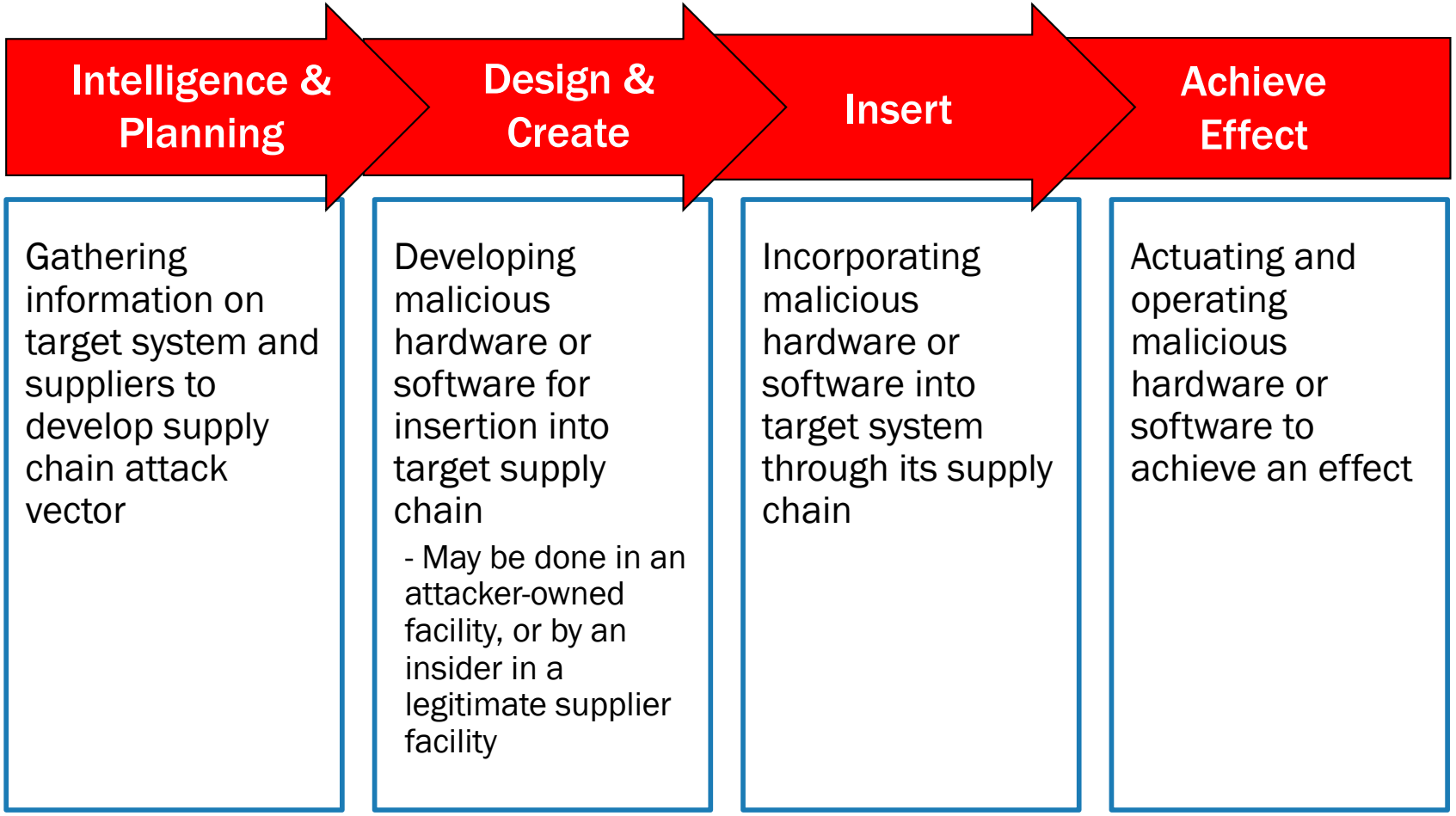
2. DoD acquisition supply chain
   - Hardest target for malicious insertion
   - Successful attack can create precise, impactful effects

3. DoD sustainment supply chain
   - A primary attack vector for fielded systems
   - Malicious insertion easier than acquisition chain
     - Reliance upon diverse and dispersed commercial sources
     - Exposure via continuing demand for obsolete parts
   - Less programmatic oversight
   - Provenance harder to track
   - Successful attack creates precise, impactful effects

The DoD sustainment supply chain is the most attractive target for sophisticated adversaries

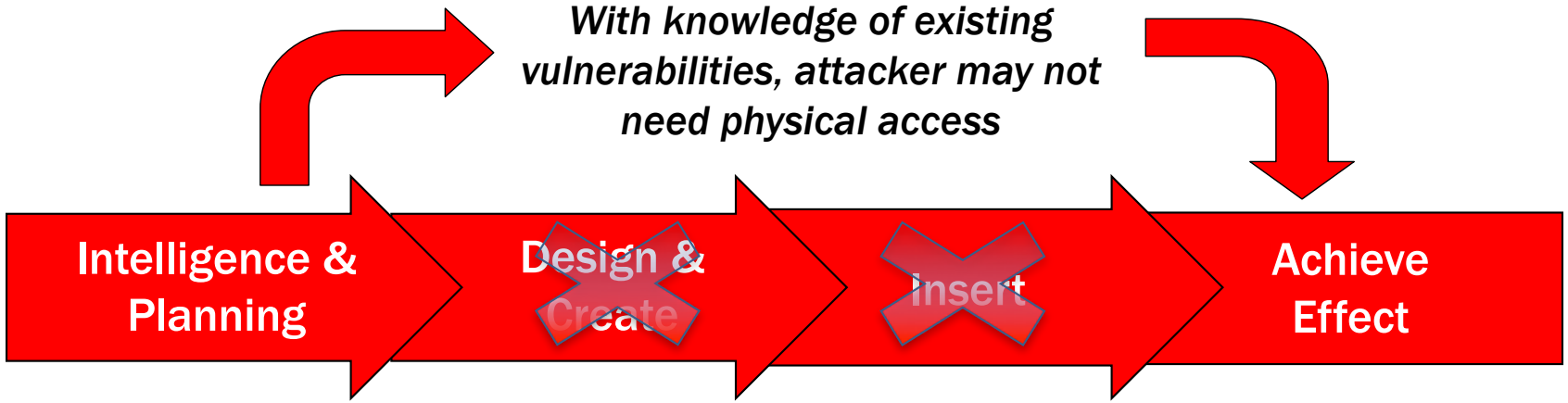
Malicious insertion is a multi-step process

Actions an attacker takes to perform a malicious insertion:

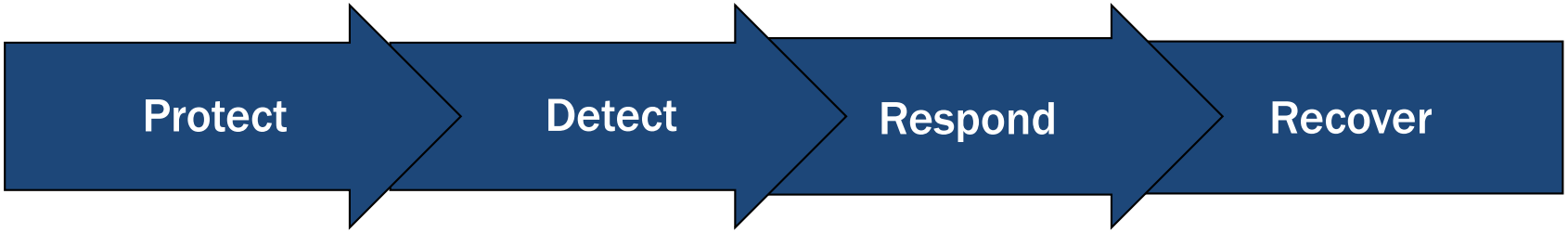


Key Observations
Exploiting existing latent vulnerabilities can bypass expensive, time-consuming steps

- Systems fielded today will make up ≥ 80% of military capability through 2025
  - "Static targets" are in the field for many years with same parts
  - Vulnerabilities can be discovered throughout life of weapon systems
- Extremely difficult to deny adversary this targeting knowledge
  - DoD uses mostly globally available, cost-effective COTS parts
  - System requirements are public in sustainment solicitations
  - Known exfiltration – "the horse has left the barn"



Mitigating Supply Chain Exploitation



- Supply chain vulnerability can be reduced by:
  - Protecting design and supplier information
  - Protecting design, manufacturing, and distribution systems
  - Employing better assurance, diverse design with built-in active monitoring and surveillance with rapid upgrade capability
- In addition, we must prepare to:
  - Identify vulnerabilities
  - Detect the exploitation
  - Respond (fight through)
  - Recover (restore system to trusted state)

Summary of Recommendations

Five categories for improvement

1. Understand supply chain risk
   - Expand vulnerability assessments
2. Mitigate potential vulnerabilities
   - Improve detection and reporting
3. Approach acquisition differently
   - Enhance program protection planning
   - Improve timeliness of supplier vetting
   - Improve system engineering
   - Use JFAC and JAPEC effectively
   - Consider cybersecurity impact of COTS products and components
4. Support life-cycle operations
   - Establish sustainment PPPs for fielded systems
   - Collect and act on parts vulnerabilities
5. Pursue technical solutions

Summary

- DoD weapons systems are at risk from:
  - Exploitation of malicious insertions
  - Malicious exploitation of latent vulnerabilities
- Active search for vulnerabilities using Cyber Awakening exercises can:
  - Identify, classify, and share vulnerabilities
  - Inform training needs
- Effective use of expert resources will improve Program Protection Plans
  - Acquisition
  - Sustainment
- Fielded systems must be supported with effective Program Protection Plans