Trusted Microelectronics Workshop:

“Hardware Assurance for the Lifecycle: The Benefits of Trusted Microelectronics”

February 26, 2015
Hosted by the National Defense Industry Association Event 587D
Acknowledgments

This workshop came together with the help of a number of important people. Britt Bommelje and Rebecca Danahy of the NDIA did a great job organizing and hosting the event. Stewart Ocheltree and the staff of BAE Systems are thanked for again providing a wonderful site to hold this workshop. Keynotes speakers Mr. John Medlin of DASD (Materiel Readiness) who spoke about important life cycle issues and Dr. Brian Cohen of the Institute for Defense Analyses (IDA) who spoke about ongoing efforts to get a better understanding of the landscape of standards and practices related to trustworthy suppliers. A panel session focused on DMSMS issues and open discussion was held with panel members including Brent Bolner (NAVSEA), Alan Howard (Wyle F-35 DMSMS), Matt MacGregor, (USAF F-35 ), Dr. Jay Mandelbaum (IDA), Joe Spruill (Lockheed Martin Corporation) and Dr. Nick Avdellas (LMI). Attendee participation has been key to the workshops’ successes and thanks go to the participants who were very active in the discussion during the event. Finally, the efforts of Dr. Brian Cohen (IDA); Sydney Pope of Decisive Analytics Corporation (DAC); and Catherine Ortiz of Defined Business Solutions really helped the workshop run smoothly.
Contents

1. Introduction ..................................................................................................................4
2. Minutes of the Workshop ............................................................................................7
   A. The Importance of DoD Lifecycle Sustainment Planning ........................................7
   B. Trustworthy Suppliers Framework ...........................................................................8
   C. DMSMS Expert Panel and Open Discussion ..............................................................10
3. Summary ....................................................................................................................14
   Appendix A : Agenda ........................................................................................................15
   Appendix B : Life-Cycle Sustainment Planning: Shift Happens, John Medlin ..........16
   Appendix C : A Framework for Understanding Trustworthy Suppliers, Brian Cohen ....68
   Appendix D : Attendees .................................................................................................86
1. Introduction

The NDIA Trusted Microelectronics Workshop series was launched in 2013 to provide an open forum for Government and Industry participants to discuss microelectronics supply and security issues related to defense and national security systems. The initial workshop held in June 2013 explored how to make the Department of Defense Instruction 5200.44 a success. The report from that meeting\(^1\) recorded a strong desire by the participants to follow up that first workshop with similar events.

A subsequent meeting was held in January 2014\(^2\) with the theme of “Trusted Microelectronics for Systems Security.” There were a number of areas identified for further discussion including opportunities for managing supply chain risk beyond Application Specific Integrated Circuits (ASICs) and opportunities for cost effectively leveraging industrial capabilities.

In August 2014, the third Trusted Microelectronics Workshop\(^3\) explored the overlap between the requirements of safety, quality and security in aerospace and defense systems. The audience presented good approaches to leverage existing quality and safety disciplines to address supply chain risks.

The most recent Trusted Microelectronics Workshop, held in February 2015, was designed to consider hardware assurance challenges in a system’s sustainment phase, as components are more difficult to get from the original suppliers. We invited sustainment managers and representatives from the Diminishing Manufacturing Sources and Material Suppliers (DMSMS) community to hear how using trusted and trustworthy suppliers can mitigate their electronic component risks later in the lifecycle. The workshop was advertised publicly and key groups of Government and industry were invited to participate. The Trusted Microelectronics Workshop description is as follows:

*NDIA is pleased to offer our fourth workshop designed to identify ways in which Trusted Microelectronics can contribute to greater systems security and information assurance. In this half-day workshop, we plan to continue the dialogue between Government and Industry on the challenges for comprehensive supply chain risk*

---

management and program protection. With participation from both Government and Industry, our workshops have provided an effective forum for direct discussions of the challenges faced by policy makers, program managers, systems developers, and supply chain managers.

Specifically we will address: How can Trusted Microelectronics provide better hardware assurance throughout a system’s lifecycle? How can DMSMS strategies consider the benefits of using Trusted Microelectronics? How can industry better engage with government programs for sustainment solutions?

Who should attend: Government and Industry program managers, systems engineers and developers, microelectronics designers, supply chain and sustainment officials, purchasing and procurement professionals, product managers and operations analysts.

Representatives from the Trusted Suppliers Steering Group will be on hand to describe how they can address the challenges faced by Government program managers. The Trusted Suppliers Steering Group is a self-formed alliance of companies that have been accredited by Defense Microelectronics Activity (DMEA) to provide Trusted Microelectronics products and services to Government programs. The Group consists of Aeroflex Corporation, BAE Systems Inc., Cypress Semiconductor Corporation, Honeywell International Inc., Intrinsix Corp, Jazz Semiconductor Trusted Foundry, ON Semiconductor, Photronics Inc., and Teledyne Technologies, Inc.

Dr. Brian Cohen (IDA), opened the workshop with an introduction to the day’s theme of exploring issues revolving around Trusted Microelectronics and system lifecycle including sustainment, risks and counterfeits. Dr. Cohen stated that DoDI 5200.44 challenges people in the acquisition community to consider sustainment issues in their program planning, and how acquisition can decisions limit sustainment options, particularly with electronics components. More closely linking acquisition and sustainment could mitigate risk in the supply chain.

Mr. John Medlin, Materiel Readiness Policy and Space Systems Portfolio Analyst, Office of the Deputy Assistant Secretary of Defense for Materiel Readiness, provided the keynote presentation on the importance of trusted electronics in defense networks and systems. The title of his presentation was “Shift Happens.” He talked about the need to do a better job addressing the transition between program protection planning, which begins early in the system acquisition process, and life-cycle sustainment planning for protecting the system and its critical components after it is deployed.

The next speaker was Dr. Brian Cohen. He introduced the work being done by the Trusted Suppliers Working Group to construct a framework that will help program managers in making decisions about product or supplier risk. (This activity was established as a direct response to issues that were raised at the three previous
Trusted Microelectronics Workshops). The title of his talk was “A Framework for Understanding Trustworthy Suppliers Throughout the Lifecycle.” Dr. Cohen described the work of the group at defining trust and what are trustworthy suppliers.

After a break that allowed attendees to hear about a new system on counterfeit detection developed by Battelle’s Larry House and SMC’s Tom Sharpe, the workshop reconvened with a panel of Government and Industry DMSMS experts. Mr. Sydney Pope of DAC and Dr. Cohen moderated a discussion during which the panelists addressed questions both from the moderators and from the attendees. The full agenda is shown in 3.Appendix A. The keynote presentation from Mr. Medlin is in 3.Appendix B and Dr. Cohen’s presentation is 3.Appendix C. The registration roster is provided in 3.Appendix D. Please note, however, that not all of those who registered were able to attend due to a snowstorm the morning of the workshop. Despite the weather challenges, more than 50 people participated and contributed to a valuable discussion.
2. Minutes of the Workshop

On Thursday, February 26, 2015 the National Defense Industrial Association (NDIA) sponsored a Trusted Microelectronics Workshop with technical co-sponsorship by the Trusted Suppliers Steering Group at the BAE Systems Facility in Washington, DC. Fifty-three individuals from Government and industry attended. A copy of the Agenda is in Appendix A. The Workshop began at 8:30 a.m. and adjourned at 12:30pm.

Welcome

Dr. Brian Cohen, Research Staff Member
Institute for Defense Analyses

Dr. Brian Cohen, Research Staff Member at the Institute for Defense Analyses, kicked off the workshop by describing this goal and then introducing the keynote speaker, Mr. John Medlin, Materiel Readiness Policy and Space Systems Portfolio Analyst, Office of the Deputy Assistant Secretary of Defense for Materiel Readiness.

A. The Importance of DoD Lifecycle Sustainment Planning

Mr. John Medlin, Materiel Readiness Policy and Space Systems Portfolio Analyst
Office of the Deputy Assistant Secretary of Defense for Materiel Readiness

Mr. Medlin started his presentation by emphasizing his belief in the need for Trusted Microelectronics. The lack of connection between the acquisition and sustainment communities create unnecessary risks in defense systems and networks. The people working in the depots and Defense Logistics Agency (DLA) most acutely understand the critical items issues.

Mr. Medlin described the challenge of trying to create a good, coherent message from all the lifecycle and sustainment activities that can be communicated to the acquisition community. Contributing to the communication challenge is the pace of obsolescence with electronic systems.

Specifically, Mr. Medlin discussed the gap between program protection plans (PPP) (an acquisition activity) and the lifecycle sustainment plans (LCSP) used by the materiel readiness community. The PPP is the seminal acquisition document – and every section of the PPP has implications for sustainment. While the PPP has guidance and policy requirements for using trusted suppliers to reduce risk, the LCSP is adding a sub-section (Section 11.1) to expressly require trusted issues to be addressed.

Mr. Medlin outlined the work that should be done to better connect the acquisition and sustainment activities; specifically we should determine:
• How does PPP relate to LCSP?
• Who is responsible for ensuring sustainment issues are addressed in the PPP?
• Who do you have to convince about the “burning platform” for trusted systems?
• What data can be used by sustainment managers to demonstrate the problem?

In closing his prepared remarks, Mr. Medlin asserted that the current logistics reassignment process fosters an “us” and “them” mentality. There is limited communication from the acquisition community to the sustainment community of the problems, even at the classified level. Establishing new communication paths across all stakeholders is the first step in solving sustainment challenges. To help promote communications, PPPs and LCSPs need to lay out how acquisition and sustainment communities support each other in maintaining program protection at each life-cycle phase. Every section of the PPP has something that needs to be addressed during sustainment; therefore, it is important systems engineers and logisticians share a mutual understanding of DMSMS risks and malicious supply chain threats.

In response to questions from the audience, Mr. Medlin identified areas for continued discussion:

• Counterfeiting was of concern to DMSMS community because of the obsolescence issue but it is a supply chain issue. What should we be doing there? Counterfeits are not just a piece part issue for logisticians and malicious insertions are malicious insertion is not just an issue for the program manager. That is because counterfeit insertion can occur anytime and anywhere and malicious insertions are a form of counterfeit.
• Resourcing DMSMS is not a viable option under the current organization structure because ASD(L&MR), DASD(SE), CIO, ASD(R) all have pieces of the problem. How can senior leadership be approached to understand the problem and the importance?
• Successful commercial programs operate under a DEVOPS (development and operations) that is a continuous lifecycle. Does it make sense for DoD programs to operate in a similar manner?

B. Trustworthy Suppliers Framework

Dr. Brian Cohen, Research Staff Member
Institute for Defense Analyses
Dr. Cohen introduced the Trusted Suppliers Working Group that formed to help program officers looking for appropriate standards and practices to include in their Program Protection Plans (PPPs) that might be relevant to addressing the need for trusted microelectronics. This ad hoc working group is putting together a framework with definitions and dimensions using a systems engineering approach to promote hardware (HwA) and software (SwA) assurance in weapon and information management systems. (Initial work of the group is focused on HwA, but later efforts may expand to include SwA.) Building from the issues raised at the third NDIA Trusted Microelectronics Workshop, the working group is identifying controls for quality, security and safety at the product component level, with a goal of creating a toolbox for program offices to select appropriate controls from recognized standards and practices.

The working group believes that system level trust (or security) is affected by a combination of component level quality, security and safety. And further that defects can be either unintended or intended and that product trustworthiness depends in part on trustworthy suppliers. The members are considering a number of industry standards and Government practices that offer product and process controls for promoting system and component level trust and for assessing supplier trustworthiness. NIST 800-161 is of special interest at a generic an overarching level as well as NIST 800-160 and NIST 800-53A R4. (DoDI 8510.01, Cybersecurity references 800-53A R4, which references 800-161.)

Dr. Cohen stated that the NIST Special Publication 800-161 was selected as the foundation for the working group’s assessment and will be the basis for a framework. As each particular standard or practice has elements and the resulting toolbox is intended to employ this framework to provide an overview of how all these standards and practices addresses counterfeiting prevention and supply chain risk management. The working group believes that although NIST “controls” were developed to promote information assurance and cyber security, some of them are also useful for promoting HwA.

In response to questions from the audience, Dr. Cohen offered the following clarifications:

- FY2012 NDAA Section 818 and DoDI 5200.44 have different definitions for trust and trustworthiness. The working group will provide a common definition.
- Consideration has to be made as to the trustworthiness of both the product and the supplier. A product from a reputable supplier could have a feature that allows vulnerabilities to be introduced into a system. But, there is an understanding that a system can never be 100% free from vulnerabilities.
- While the activity has involved Government and their support contractors so far, involvement by industry will be essential to achieve success.
Government leadership will determine how and when to engage with industry.

C. DMSMS Expert Panel and Open Discussion

Panel discussion moderated by Mr. Sydney Pope, Decisive Analytics Corporation, Support Contractor to the Office of the Deputy Assistant Secretary of Defense for Systems Engineering (ODASD(SE)) and Dr. Brian Cohen, Research Staff Member, Institute for Defense Analyses

Panelists

- Brent Bolner, Manager, NAVSEA DMSMS
- Alan B. Howard, F-35 DMSMS Lead, OUSD (AT&L), F-35 DMSMS
- Matt MacGregor, Program Manager, F-35 DMS and Affordability
- Dr. Jay Mandelbaum, Research Staff Member, Institute for Defense Analyses
- John Medlin, Materiel Readiness Policy and Space Systems Portfolio Analyst, Office of the Deputy Assistant Secretary of Defense for Materiel Readiness
- Joe Spruill, CSCP, Principal, Logistics and Sustainment, Corporate Engineering & Technology, Lockheed Martin Corporation

The panelists made opening remarks generally concluding that:

- Better communication and more involved leadership are needed.
- The acquisition community does not recognize the problems their decisions create for a system’s sustainment phase. DMSMS considerations (parts management) should be addressed in the PPP process including planning for both Government and contractors responsible for providing lifecycle support. DMSMS is rarely fully funded. A more honest assessment of sustainment costs should be included early in the program’s development and should strategically address DMSMS by considering cost savings/avoidance over the lifecycle.
- DMSMS issues will likely get even more complicated in the future; integrating language and instructions into contracts will be crucial.

Mr. Pope followed the opening statements with the question, “Why aren’t the Services more focused on PPP and its inclusion of parts planning?”
A general consensus was that:

- OEMs & primes are responsible for providing the parts. Earlier, programs had success when they instructed the systems integrators to manage the system at the piece part level.

- There is a greater need for top-level understanding of the complexities of DMSMS and parts obsolescence.

The discussion transitioned to technical data packages with some opinions offered as follows:

- Technical data package ownership and bills of material are important for parts management and DMSMS. Having this information helps when evaluating repair or replace options – component replacement or new technology insertion.

- The space community works collaboratively with contractors to ensure technical data packages are available to those responsible for operating the systems.

- Regulatory constraints, such as requalification requirements, limit DMSMS options.

- Work is being done with software to tailor data rights agreements with contractors and to assign operational responsibility where it is most cost-effective. DoD intellectual property policy is being developed with these issues in mind.

- Owning the technical data packages/rights may be too expensive for all defense systems, and managing the contractor and competition can sometimes be a more cost-effective solution.

- Performance based agreements can help both Government and contractors.

  - Example was given of a Navy radio box that Honeywell took over lifecycle management for. Initially, there were many radio box configurations with no two systems alike. Honeywell replaced all boxes with one configuration and created the software to address any legacy issues. In addition, Honeywell streamlined the process for making future box upgrades, which was highly cost-efficient for the Navy and for Honeywell.

The next discussion item focused on the state of technical roadmaps. Some opinions offered included:
• Not much technology road mapping is currently being done; however, programs should plan for technology refreshments to take full advantage of nonrecurring engineering (NRE) opportunities.

• Planned modernization programs need to be part of an overall system-engineering plan in the beginning of the program acquisition process.

Dr. Cohen followed the discussion with the question, “Can Trusted microelectronics help with electronics obsolescence since obsolescence increases the risk of counterfeit problems?” Some opinions offered included:

• Trust is a much harder problem in this era of global supply chains. In the past, most original equipment manufacturers (OEMs) had robust supply chains and inspection and engineering groups, which today no longer exist. The onus has been put on Government program offices to understand the components being installed in their systems.

• There is a need to have better connection between DMSMS functions and those functions responsible for addressing counterfeit prevention; the two groups are not necessarily connected depending on where they reside within their respective organizations.

• There is a mismatch between commercial and defense industry’s lifecycles. When commercial off the shelf (COTS) consumer electronics are used in a defense system, the systems need to be built to be disposed in a way that eliminates the need to be concerned about DMSMS.

• Sophisticated reverse engineering capabilities exist within the Government at Defense Microelectronic Activity (DMEA) and Department of Energy (DOE) Kansas City Plant that could be cost effective for replacing obsolete electronic parts.

Dr. Cohen followed the discussion with the question, “Are there opportunities for collaboration for parts that could solve obsolescence and trust issues? If there is a common piece of hardware across several programs, can we deal with the DMSMS once for all?” Some suggestions offered included:

• Program realignment would be needed to handle DMSMS across programs – need to link DMSMS, PPP and counterfeit strategies.

• Open industry standards could solve commonality issues and organizations like the joint Electronic Device Engineering Council (JEDEC) could help.

• With the small size of the defense-aerospace electronics market, needs aggregation would help suppliers forecast and meet demand.
• Defense Logistics Agency (DLA) uses parts registration to identify parts common across multiple programs but it could be used more effectively.

• The space community has a system called Parts Units Material Processes Systems (PUMPS) that allows space organizations to see parts used across space hardware. PUMPS is being used to enable aggregating Field Programmable Gate Array (FPGA) buys to save $5-6m procurement dollars. PUMPS is managed by the systems engineering organizations.

Mr. Pope invited the panelists to give concluding remarks that are summarized below:

• To fix DMSMS we need to better define the problem, the stakeholders, and develop an outreach program.

• Consider developing a policy of open systems, sustainment, system engineering and technology refresh that involves industry involvement and competition.

• DMSMS is a symptom of a much larger problem; get systems engineers and supply chain managers involved early to eliminate the need for DMSMS.

• Systems engineering can make trades early in a system’s development. We need to study the successes and find the balance with sustainment, logistics and acquisition.

• Develop leaders that manage a program from cradle to grave and treat the problem for what it is – a matter of National Security.
3. Summary

This workshop brought Government and industry together to discuss the continuing impact of the DoD policy on Trusted systems and supply chain management (DoDI 5200.44) and explored areas for synergy with long-standing safety and quality initiatives. A series of productive exchanges between Government and industry took place. Industrial representatives heard, sometimes for the first time, how the Government’s systems engineering organizations work to protect their systems from risks beyond the intentional tampering threats addressed by Trusted Suppliers.

The participants generally had pervasive concerns about the dependence on microelectronics technologies and products that are increasingly driven by global commercial markets. This continues to cause movements of industry and intellectual property overseas posing risks to defense interests. While there is a clear understanding of these issues by most of the workshop participants, this understanding is still being disseminated to the vast majority of the acquisition enterprise.

There was a fruitful discussion on the value of exploring ways in which Trusted Microelectronics can benefit the safety and quality efforts; and how safety, quality and security requirements may be combined for improved mission assurance with a reduced administrative burden.

There was agreement that hardware assurance with electronics and microelectronics components is an emerging concern that touches quality, safety, and security. Engineering expertise to consider hardware assurance during the system design phase needs to be developed to realize the greatest benefits.

The connection between safety, quality and security was felt to warrant further discussions and might warrant the creation of a working group and/or further workshops.

The attendees were uniformly very positive about the meeting and interest was shown in holding a similar event in the near future.
Appendix A: Agenda

TRUSTED MICROELECTRONICS WORKSHOP

8:30am – 8:35am  WELCOME
Dr. Brian Cohen, Research Staff Member, Institute for Defense Analyses

8:35am – 9:20am  THE IMPORTANCE OF DOD LIFECYCLE SUSTAINMENT PLANNING
Mr. John Medlin, Materiel Readiness Policy and Space Systems Portfolio Analyst, Office of the Deputy Assistant Secretary of Defense for Materiel Readiness

9:20am – 10:00am  TRUSTWORTHY SUPPLIERS FRAMEWORK
Dr. Brian Cohen, Research Staff Member, Institute for Defense Analyses

10:00am – 10:15am  NETWORKING BREAK

10:15am – 12:30pm  DMSMS PANEL & OPEN DISCUSSION BETWEEN GOVERNMENT & INDUSTRY
MODERATORS:
► Mr. Sydney Pope, Systems Engineering Security Expert, Decision Analytics Corporation
► Dr. Brian Cohen, Research Staff Member, Institute for Defense Analyses

PANELISTS: GOVERNMENT
► Mr. Brent Bolner, Manager, NAVSEA DMSMS
► Mr. Alan Howard, Lead, OUSD (AT&L), F-35 DMSMS
► Mr. Matt MacGregor, Program Manager, F-35 DMS & Affordability
► Dr. Jay Mandelbaum, Research Staff Member, Institute for Defense Analyses

PANELISTS: INDUSTRY
► Mr. Joe Spruill, CSCP, Principal, Logistics and Sustainment, Corporate Engineering, Technology & Operations, Lockheed Martin Corporation
► Dr. Nick Ardellas, Program Manager, LMI Maintenance & Readiness

12:30pm  ADJOURN
Life-Cycle Sustainment Planning

Trusted MicroE Workshop
February 26, 2015
Agenda

- Introduction
- Shift Happens
- LCSP and PPP
- PPP Elements With Sustainment Areas of Interest
- What’s The Problem
- Life Cycle Activities
- Communication
- Conclusion

He Who Fails To Plan is Planning To Fail

Operations & Support 60-75% of Life Cycle Cost!
What I Perceive
Program Protection Plan (PPP)

Life Cycle Sustainment Plan (LCSP)
### LCSP and PPP Elements

#### 11 Additional Sustainment Planning Factors

<table>
<thead>
<tr>
<th>LCSP</th>
<th>PPP</th>
</tr>
</thead>
</table>
| **List additional sustainment issues** or risks that cross functional lines that could adversely impact sustainment or sustainment support across the system’s life cycle** that are not included elsewhere in the LCSP. If the topic is addressed in another document (e.g., the Systems Engineering Plan, etc.) provide a short summary and reference the source. For example:  
  • **Critical Program Information elements provided in the Program Protection Plan (maintaining anti-tamper on component or sub-components)**  
  • Materials with environmental impacts addressed in the PESHE (require special handling, demilitarization, facilities, training)  
  • System integration with or onto another platform (vehicles onto transport ships/RoRos, air transports, etc.)  
  • Integration of C4I with the system. | **9.4. Sustainment**  
  How will Program Protection requirements and considerations be managed in sustainment?  
  Who is responsible for this?  
  Link to the relevant Lifecycle Sustainment Plan (LCSP) language. |
Reality Check

What I Thought

What I Got

PPP

LCSP

[Image of a person pouring water over their head]
PPP Elements With Sustainment Interest

- **2.0. Program Protection Summary**
  - 2.1. Schedule

- **2.2. CPI and Critical Functions and Components Protection**

- **5.0. Threats, Vulnerabilities, and Countermeasures**
  - 5.1. Threats
  - 5.2. Vulnerabilities
  - 5.3. Countermeasures
    - 5.3.1. Anti-Tamper (AT)
    - 5.3.2. Information Assurance (IA)
    - 5.3.3. Software Assurance
    - 5.3.4. Supply Chain Risk Management (Trusted Suppliers, Counterfeit)
    - 5.3.5. System Security Engineering
    - 5.3.6. General Countermeasures

Assumption: The PPP, et al, is the seminal acquisition document
6.0. Other System Security-Related Plans and Documents

7.0. Program Protection Risks

8.0. Foreign Involvement

9.0. Processes for Management and Implementation of PPP
   - 9.1. Audits/Inspections
   - 9.2. Engineering/Technical Reviews
   - 9.3. Verification and Validation
   - 9.4. Sustainment
     - How will Program Protection requirements and considerations be managed in sustainment? Who is responsible for this?
     - Link to the relevant Lifecycle Sustainment Plan (LCSP) language.

10.0. Processes for Monitoring and Reporting Compromises

11.0. Program Protection Costs
   - 11.1. Security Costs
   - 11.2. Acquisition and Systems Engineering Protection Costs
What’s the Burning Platform?
Building IA into requirements development and system design.
Transition from Configuration to Parts Management

Acquisition Process

Logistics Reassignment Process
- Governed by DoD 4140.26M (Vol 2 & 4)
- Service defines criticality of part or item
  - Critical Flight Safety
  - Critical Application
- Service defines Acquisition Strategy:
  - Sole source
  - Competitive bid

Sustainment Process

Service Requirements

Service Engineering Support Activity (ESA) retains configuration control (Tech data)

Integrated Materiel Management

Wholesale management of consumable items

US

THEM

Operating Force (Operational Weapon Systems through DEMIL & Disposal)

DoD 4140.26M DoD Integrated Materiel Management (IMM) for Consumable Items
Communication Is The Key

Everyone must communicate, align, and integrate disparate, stovepiped, functional area stakeholder requirements to formulate, implement, execute and sustain systems across its life cycle.

Both Teams Are Playing Football

...but they are not playing the same game.

We, DoD, consistently fail to fully communicate with ALL stakeholders.
Communication
Questions
BACK UP
2.0. Program Protection Summary

2.1. Schedule

A Program Protection schedule overlaid onto the program's master schedule (milestones, systems engineering technical reviews, etc.) includes:

- Countermeasure (e.g. Anti-Tamper, Information Assurance) testing/verification events

Countermeasure testing/verification events are not one-time activities but occur across the system’s life-cycle

- Are these accounted for in O&S cost estimates; how is the PPP carried forward/monitored; who in sustainment manages PPP/countermeasure requirements; what are schedule events in Post MS-C and O&S Phase?
2.2. **CPI and Critical Functions and Components Protection**

- Over the lifecycle of the program list all CPI and critical functions and components (including inherited and organic) mapped to the security disciplines of the countermeasures being applied in Table 2.2-1 below.

- Does inherited or organic functions and components bring a separate O&S cost to maintain; are there MOA/MOUs;
  - See Section 3.1, 3.2, 3.3
PPP Areas of Interest for Sustainment

- Table 2.2-1: CPI and Critical Components Countermeasure Summary

- Is the implementation of countermeasures across the system’s life-cycle identified, understood, and managed?
  - Has the impact on IPSEs; O&S costs; etc, been identified?
Table 2.2-1: CPI and Critical Components Countermeasure Summary (mandated) (sample)

<table>
<thead>
<tr>
<th>#</th>
<th># Inherited and Organic</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Algorithm QP</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>System Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Configuration Encryption Hardware</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IDS Policy Configuration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>IDS Collected Data</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>KGV-1368</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>iDirect M161T Hub-Line Card</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Cisco Router IOS with Advance Security Option (ASO)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**KEY** [Examples Included: UPDATE THIS LIST ACCORDING TO PROGRAM]

- **X** = Implemented
- **I** = Denotes protection already implemented if CPI is inherited

<table>
<thead>
<tr>
<th>General CMs</th>
<th>Research and Technology Protection CMS</th>
<th>Trusted Systems Design CMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Personnel Security</td>
<td>8 Transportation Mgmt</td>
<td>11 IA/Network Security</td>
</tr>
<tr>
<td>2 Physical Security</td>
<td>9 Anti-Tamper</td>
<td>12 Communication Security</td>
</tr>
<tr>
<td>3 Operations Security</td>
<td>10 Dial-down Functionality</td>
<td>13 Software Assurance</td>
</tr>
<tr>
<td>4 Industry Security</td>
<td></td>
<td>14 Supply Chain Risk Management</td>
</tr>
<tr>
<td>5 Training</td>
<td></td>
<td>15 System Security Engineering (SSE)</td>
</tr>
<tr>
<td>6 Information Security</td>
<td></td>
<td>16 Other</td>
</tr>
<tr>
<td>7 Foreign Disclosure/Agreement</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.0. Threats, Vulnerabilities, and Countermeasures

- Summarize any identified threats and vulnerabilities to CPI and critical functions/components in Table 5.0-1 below. Also identify any countermeasures selected to mitigate risks of compromise.

Table 5.0-1: Summary of CPI Threat, Vulnerabilities, and Countermeasures

- Has the impact on IPSEs; O&S costs; etc, been identified?
Table 5.0-1: Summary of CPI Threat, Vulnerabilities, and Countermeasures (mandated) (sample)

<table>
<thead>
<tr>
<th>CRITICAL COMPONENTS</th>
<th>CPI/CC (and CC supplier) Section 2.0</th>
<th>Threats Section 5.1</th>
<th>Vulnerabilities Section 5.2</th>
<th>Countermeasures Section 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDirect M1D1T Hub-line Card</td>
<td>2, 8, 9, 14</td>
<td>3</td>
<td>Communication Security; Software Assurance; SCRM</td>
<td></td>
</tr>
<tr>
<td>Cisco Router IOS with ASO</td>
<td>2, 6, 8, 9, 14</td>
<td>4</td>
<td>Supply Chain Risk Management</td>
<td></td>
</tr>
<tr>
<td>CPI</td>
<td>Algorithm 4, 5, 7, 13-15</td>
<td>1,2</td>
<td>Anti-Tamper, SSE, Supply Chain Risk Management</td>
<td></td>
</tr>
<tr>
<td>System/Security Configuration</td>
<td>1, 9, 14, 15</td>
<td>1</td>
<td>Secure storage of configuration; Supplier Assurance</td>
<td></td>
</tr>
<tr>
<td>Encryption Hardware</td>
<td>2, 9, 14</td>
<td>2</td>
<td>Supply Chain Risk Management, NSA encryption device</td>
<td></td>
</tr>
</tbody>
</table>
5.1. Threats

- Table 5.1-1: Threat Product References
  
  **Expectations: As threat products are received, reference these documents in Table 5.1-1. This table should be comprehensive by Milestone B. For the Supply Chain Threat Assessments, document each critical component supplier (or potential supplier) that has been assessed.**

Supply Chain Risk Management is an evolving and growing area of interest and concern.

- Has the program assessed the current SCRM environment and evaluated the impact on IPSEs, O&S cost, etc?
<table>
<thead>
<tr>
<th>Title of Program-Specific or Other Threat Products Used for PPP Threat Analysis</th>
<th>Classification</th>
<th>Document Date</th>
<th>Organization(s) Producing the Product</th>
<th>Reference/Link to Product</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FORMAL THREAT REPORTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFOSI Counterintelligence Assessment/Report</td>
<td>S</td>
<td>Jul 2002</td>
<td>HQ Office of Special Investigations</td>
<td></td>
</tr>
<tr>
<td>AFOSI Department of Defense Threat Assessment</td>
<td>S</td>
<td>Dec 2007</td>
<td>Office of Special Investigations</td>
<td></td>
</tr>
<tr>
<td>Capstone Threat Assessment (CTA)</td>
<td>U-S</td>
<td>Dec 2002</td>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td>Foreign Technology Assessment</td>
<td>U</td>
<td>Feb 2004</td>
<td>Counterintelligence Service</td>
<td></td>
</tr>
<tr>
<td>Integrated Threat Assessment (ITA)</td>
<td>U-S</td>
<td>Jan 2002</td>
<td>Service for Special Assess Programs</td>
<td></td>
</tr>
<tr>
<td>Technology Targeting Risk Assessment (TTRA)</td>
<td>U-S</td>
<td>Mar 2006</td>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td>System Threat Assessment Report (STAR)</td>
<td>S</td>
<td>Jan 2007</td>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td><strong>SUPPLY CHAIN THREAT ASSESSMENTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iDirect M1D1T Hub-line Card Assessment</td>
<td>TS/SCI</td>
<td>Apr 2009</td>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td>Cisco Router IOS with ASO</td>
<td>TS/SCI</td>
<td>Apr 2009</td>
<td>Defense Intelligence Agency</td>
<td></td>
</tr>
<tr>
<td><strong>OTHER THREAT DOCUMENTS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.2. Vulnerabilities

- How will the program identify new vulnerabilities (both system-level and in the development environment) to the CPI and mission-critical functions and components?

- Who is responsible for doing this, and with what frequency? Include the responsible person in the table in Section 1.2.

- How often will vulnerabilities be re-assessed?

- How will identified vulnerabilities be mitigated?

- Is the vulnerability re-assessment included in the O&S cost estimate [not a cheap endeavor]?
  - Identified re-assessment cycle schedule, red teams, etc
5.3. Countermeasures

- Succinctly describe the implementation of each countermeasure used to protect CPI and critical functions and components. Be specific: If SCRM Key Practices apply, describe which ones; if using Software Assurance techniques, explain which ones.

- Does implementation planning address protection across the system’s life-cycle; Are Software Assurance techniques addressed as part of the software IPSE; included in O&S cost estimates; etc
5.3.1. Anti-Tamper (AT)

- Who will identify AT requirements and who is responsible for developing an AT plan? When will the AT Plan be completed? Include plans for engaging with the Component AT lead and Executive Agent for AT.
  - If an AT Plan or AT Plan Waiver has been developed, submit as an Appendix.

- Did the PSM or staff review/coord on the AT Plan; does the waiver require periodic review—who is OPR in sustainment; are there sustainment impacts or risks due to the waiver?
5.3.2. Information Assurance (IA)

• Expectation: IA countermeasures planning should account for the system being acquired and any support information systems that may contain or host CPI and critical functions and components. The Acquisition IA Strategy documents the plan for implementing IA specifically on the system being acquired. IA controls can also be applied to protect CPI and critical functions and components as they are handled/transmitted across contractor or partner systems.

How do countermeasures impact IPSEs; are there O&S cost impacts: who is the responsible office or person in sustainment (Sys Eng/Sust Eng; PSM; ?);
PPP Areas of Interest for Sustainment

5.3.3. Software Assurance

- Who is responsible for Software Assurance?
- How will COTS software and software of unknown pedigree (i.e., software from sources buried in the supply chain) be protected and tested/vetted?

- Who has Software Assurance responsibilities in sustainment—is there a transition plan; are COTS tech refresh and Software Assurance requirements identified; are there O&S cost estimates; are contracts in place for PPP contractors; are organic organizations ready, etc?
5.3.4. Supply Chain Risk Management

- How will the program manage supply chain risks to CPI and critical functions and components?
- Explain how supply chain threat assessments will be used to influence system design, development environment, and procurement practices. Who has this responsibility? When will threat assessments be requested?

Who is responsible for supply chain risk management in sustainment; when will threat assessments be updated; are impacts to Supply Support (SCRM) identified;
5.3.4. Trusted Suppliers

- Will any ASICs require trusted fabrication?
- How will the program make use of accredited trusted suppliers of integrated circuit related services?

Are trusted foundry/ASICs included in the LCSP; are there life cycle impacts on Integrated Product Support Elements (IPSE); are SCRM processes & procedures in place; AT considerations;
5.3.4.2. Counterfeit Prevention

- What counterfeit prevention measures will be in place? How will the program mitigate the risk of counterfeit insertion during Operations and Maintenance?

- Are there AT elements; who will manage counterfeit prevention in sustainment; what are impacts on IPSEs; is it included in the LCSP; etc?
5.3.5. System Security Engineering

- Who is responsible for system security engineering?
- Describe the linkage between system security engineering and the Systems Engineering Plan. How will system security design considerations be addressed?

Who is responsible during sustainment; what is the impact on IPSEs (Sust Eng)?
5.3.6. General Countermeasures

- Summarize generic countermeasures or security activities in place that will/do apply to all program information/facilities/personnel and contribute to the protection of CPI and critical functions and components

Impact of generic countermeasures on IPSEs; how is oversight/control in sustainment;

- COMSEC (Development Environment); OPSEC; Foreign Visit Program; CPI Protection Training; Information Assurance (Development Environment); Secure System Administration; Personnel Security; Industrial Security
6.0. Other System Security-Related Plans and Documents

- Expectation: If Technical Assistance Agreements, Memoranda of Agreement (MOA), Memoranda of Understanding (MOU), or other similar agreements have been signed, reference or link to them in an additional table with a description of the key commitments.

- Are agreements carried over/applicable in sustainment; who is OPR in sustainment;
7.0. Program Protection Risks

- Describe how Program Protection risks (cost, schedule, technical) will be integrated with overall Program risk management.

- Discuss the approach to identifying residual risks of CPI and critical function and component compromise after countermeasure implementation. Are there any unmitigated risks?

- Include a risk cube and mitigation plan for the top Program Protection risks.

- What are the mitigation actions or unmitigated risks that carry over into sustainment; who is the OPR in sustainment; is funding planned and programmed after MS-C and O&S Phase?
PPP Areas of Interest for Sustainment

8.0. Foreign Involvement

- Summarize any international activities and any plans for, or known, foreign cooperative development or sales of the system.

- Are there cooperative supply agreements via FMS (CLSSA); are there different configurations requiring control—where documented; impact on IPSEs; who is OPR in sustainment; etc?
9.0. Processes for Management and Implementation of PPP

• 9.1. Audits/Inspections
  - Summarize the timing of security audits/inspections. How will contractor security requirements be enforced? Who is responsible for this?

What audits/inspections carry over in to sustainment; are there any open audit/inspection findings that carry over in to sustainment; if set cycle, are these reflected as an O&S cost in POE, SCP, ICE; are funds planned and programmed for after MS-C and during O&S Phase?
9.0. Processes for Management and Implementation of PPP

- 9.2. Engineering/Technical Reviews
  - How will system security requirements be addressed in Systems Engineering Technical Reviews, functional/physical configuration audits, etc? Who is responsible for this?
  - What Program Protection entry/exit criteria will be used for these reviews?

- How are review findings, risks and issues carried forward after MS-C and into the O&S Phase; are modifications or upgrades addressed or planned?
9.0. Processes for Management and Implementation of PPP

- 9.3. Verification and Validation
  
  - Explain how the program will integrate system security requirements testing into the overall test and evaluation strategy. Who is responsible for this?
  
  - Link to relevant discussion in T&E documents.

For test findings, what is the process to carry forward after MS-C and into the O&S Phase; is there any testing that is planned in sustainment (FOT&E) and who is responsible; etc?
9.0. Processes for Management and Implementation of PPP

- 9.4. Sustainment
  - How will Program Protection requirements and considerations be managed in sustainment? Who is responsible for this?
  - Link to the relevant Lifecycle Sustainment Plan (LCSP) language.

- Is LCSP documentation adequate; who is the OPR in sustainment (Sust Eng?);
10.0. Processes for Monitoring and Reporting Compromises

- Summarize the plan/procedure for responding to a CPI compromise or a supply chain exploit.
- What constitutes a compromise or exploit? Who is notified if one occurs? Define what constitutes an Anti-Tamper event or a Supply Chain exploit.

Who is the OPR and where is the plan and/or procedures for CPI compromise or supply chain exploit in the sustainment; have there been any events and what corrective actions were taken;
11.0. Program Protection Costs

- Indicate where Program Protection costs are to be accounted for in the SCP and program budget. Who has the responsibility to ensure Program Protection costs are estimated and included in the programs budget and contracts?

- Did requirements informing SCP cost estimates extend into O&S; what were those costs and is the PSM aware?
11.0. Program Protection Costs

11.1. Security Costs

- Indicate/Estimate the security costs associated with Program Protection that exceed normal NISPOM costs. [National Industrial Security Program Operating Manual]
- Will SCIFs or other secure facilities require construction specifically for CPI protection?
- If limited access rosters or other similar instruments will be used, how much will development and maintenance of the roster cost?

Are excess NISPOM and access roster costs included for SCP and include O&S; are there SCIF requirements for operations & sustainment;
11.0. Program Protection Costs

- 11.2. Acquisition and Systems Engineering Protection Costs
- Table 11.2-1: Acquisition and Systems Engineering Protection Costs

What are the planned program protection costs in the O&S Phase; are these discrete elements that inform the POE, SCP & O&S cost estimate; are there planning and programming costs in POM and out years; etc?
Appendix C:
A Framework for Understanding Trustworthy Suppliers, Brian Cohen
A Framework for Understanding Trustworthy Suppliers

Brian S. Cohen
About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task DD-S-2635, “Trusted Microelectronics,” for Defense Microelectronics Activity. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Copyright Notice
© 2015 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

Acknowledgments
Huan Lin Zhang, Vashisht Sharma, Daniel J. Radack

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].
A Framework for Understanding Trustworthy Suppliers Throughout the Lifecycle

This material represents ongoing technical work and does not represent any government views.

Brian Cohen, bcohen@ida.org
703-845-6684
February 26, 2015
Team’s Scope and Objectives

- Examine how System Security integrates with System Quality and Safety and how supply chain security is related
  - Applicable to Supply Chain Risk Management and Counterfeits
- Develop a way of describing supplier and product trustworthiness
- Develop general controls* associated with supplier and product Trustworthiness
- Develop a Framework for Trustworthiness from a quality, security, and safety perspective and understand how different practices and standards contribute to “Trustworthiness”

* Controls are safeguards or countermeasures to avoid, counteract or minimize security risks
Initial Approach

- Develop Definition for “Trustworthiness” and related concepts and terms
  - Based on how component security weakness (“vulnerabilities”) may impact security aspects of System Performance and Mission Success
  - Trustworthy products depend on Trustworthy Suppliers

Trustworthiness is a basis for knowing whether a product is free from “vulnerabilities” that would compromise system or mission security

- Identify an organized and comprehensive approach to describing controls that represent a common generic way of understanding different ways to achieve product “Trustworthiness”
  - Figure out which controls make sense

- Perform an Assessment of current practices and standards that can be utilized to achieve Trustworthiness
  - Identify and review standards and organizations current approaches for the qualification of suppliers from a quality, security and safety perspective
  - Develop a framework in the context of “qualification requirements” to understand the current qualification practices and the attributes that contribute to trustworthiness in the supply chain

Goal is to enable a definition of the needed level of product and supplier trustworthiness and then enable buyers to select appropriate controls that might achieve that requirement
Component Vulnerabilities

- Non uniform and/or non random premature failure
- Inappropriate communication channels
- Input output ports that provide greater access/visibility than required to perform specified functions
- Component security feature defects
- Loss of access to supply
- Performs functions beyond those in the specification
- Component has falsified (or unknown) provenance
- Intended component features are security hazards
- Component contains functional defects (design/specification flaws)
- Component itself may contain information or technology that creates a system security issue
- Component supplier may know and reveal customer confidential information
Current Standards, Practices and Regulations

- DMEA Trusted Suppliers
- DLA Qualified Suppliers List for Distributors (QSLD)
- QTSL Program (Qualified Testing Suppliers List)
- DLA Qualified Manufacturers List (QML)
- DLA Qualified Products List (QPL)
- NASA/JPL Approved Supplier List
- MDA Distributor Qualification Program
- ISO 9000
- NISTIR-7622
- Open Group O-TTPS
- ISO/IEC 27036
- SAE/G19 – AS5553, AS6171(Draft), AS6174, AS6496, ARP 6178
- IDEA 1010
- NDAA 2015 818c
- Section 2319 of Title 10
- FAR Subpart 9.2
- **NIST SP 800-161, SP 800-53 R4 – This was identified as a foundation for the Framework**
Trustworthiness Framework Approach

- DOD’s approach is based on a Risk Management Framework for Cyber
  - DODI 8510.01 issued 3/12/14
  - Employs NIST controls as described in NIST SP-800-53
- NIST has adapted SP-800-53 to SCRM as NIST SP-800-161
  - The Trustworthiness Framework is based on 800-161
- New Risk Management (RM) Guide about to be issued
  - Team will evaluate the guide to harmonize these efforts with the new RM guide
NIST SP 800-161 Controls Families

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Planning
- Program Management
- System and Services Acquisition
- Personnel Security
- Provenance
- Risk Assessment
- System and Communication Protection
- System and Information Integrity
ICT SCRM Security Families and Controls (1)

- Access Control
  - Access control policy and procedures
  - Account management
  - Access enforcement
  - Information flow enforcement
  - Separation of duties
    - (Least privilege)
  - Remote access
  - Wireless access
  - Access control for mobile devices
  - Use of external information systems
  - Systems / components / devices
  - Information sharing
  - Publicly accessible content
  - Access control decisions

- Awareness and Training
  - Security awareness and training policy and procedures
    - (Role-based security training)

- Audit and Accountability
  - Audit and accountability policy and procedures
  - Audit events
  - Non-repudiation
  - Audit generation
  - Monitoring for information disclosure
  - Cross-organizational auditing

- Security Assessment and Authorization
  - Security assessment and authorization policies and procedures
  - Security assessments
  - System interconnections
  - Plan of action and milestones
  - Security authorization
  - Continuous monitoring

- Configuration Management
  - Configuration management policy and procedures
  - Baseline configuration
  - Configuration change control
  - Security impact analysis
  - Access restrictions for change
  - Configuration settings
  - Least functionality
  - Information system component inventory
  - Components to systems
  - Configuration management plan
    - (Software usage restrictions)
  - User-installed software

- Contingency Planning
  - Contingency planning policy and procedures
  - Contingency plan
  - Alternate storage site
  - Alternate processing site
  - Telecommunications services

- Incident Response
  - Incident response policy and procedures
  - Incident handling
  - Incident reporting
  - Information spillage response

- Maintenance
  - System maintenance policy and procedures
  - Controlled maintenance
  - Maintenance tools
  - Nonlocal maintenance
  - Maintenance personnel
  - Timely maintenance
  - Maintenance monitoring and information sharing
### Media Protection
- Media protection policy and procedures
- Media transport
- Media sanitization

### Planning
- Security planning policy and procedures
- System security plan
- Information security architecture

### Program Management
- Information security program plan
- Senior information security officer
- Information security resources
- Mission/business process definition
- Threat awareness program

### System and Services Acquisition
- System and services acquisition policy and procedures
- Allocation of resources
- System development life cycle
- Acquisition process
- Information system documentation
- Security engineering principles
- External information system services
- Developer configuration management
- Developer security testing and evaluation
- Supply chain protection
- Criticality analysis
- Development process, standards, and tools
- Developer-provided training
- Developer security architecture and design
- Tamper resistance and detection
- Component authenticity
- Customized development of critical components
- Developer screening
- Unsupported system components

### Personnel Security
- Personnel security policy and procedures
- Access agreements
- Third-party personnel security

### Provenance
- Provenance policy and procedures
- Tracking provenance and developing a baseline
- Auditing roles responsible for provenance

### Risk Assessment
- Risk assessment policy and procedures
- Security categorization
- Risk assessment

### System and Communication Protection
- System and communications protection policy and procedures
- Information in shared resources
- Denial of service protection
- Boundary protection
- From non-organizationally configured hosts
- Transmission confidentiality and integrity
- Mobile code
- Platform-independent applications
- Protection of information at rest
- Heterogeneity
- Concealment and misdirection
- Distributed processing and storage
- Out-of-band channels
- Operations security

### System and Information Integrity
- System and information integrity policy and procedures
- Flaw remediation
- Information system monitoring
- Security alerts, advisories, and directives
- Software, firmware, and information integrity
- Information handling and retention
## Identifying Which Controls are Relevant

<table>
<thead>
<tr>
<th>NIST SP 800-161 SCRM Control</th>
<th>Control Name</th>
<th>Descriptions</th>
<th>Relevant to Trustworthy Supplier WG</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCRM_AC-4(4)</td>
<td>Information Flow Enforcement</td>
<td>Physical / Logical Separation Of Information Flows</td>
<td>The organization should ensure the separation of the information system and ICT supply chain infrastructure information flow. Various mechanisms can be implemented including, for example, encryption methods (e.g., digital signing) for protecting of information as well as the management of flow control of the information where feasible. Flow control within the organizations operations may be manageable. However, addressing information flow between the organization and its system integrator, external service provider, and even supplier is likely more challenging, especially when leveraging public networks. Organizations should ensure that, at a minimum, protection measures are implemented for any appropriate data (e.g., component data and any related metadata).</td>
</tr>
<tr>
<td>SCRM_AC-5</td>
<td>Separation Of Duties</td>
<td>The organization should ensure that appropriate separation of duties is established for decisions requiring the acquisition of both information system and ICT supply chain infrastructure components. Separation of duties helps to ensure that adequate protections are in place for components entering organizations supply chain. Examples include separating technical decision makers from the procurement personnel for deciding on components in the supply chain, or having two engineers review and test component samples from multiple suppliers to ensure availability of multiple supply and standards-based standards to verify ability for components to be</td>
<td>Yes</td>
</tr>
<tr>
<td>(SCRM_AC-6)</td>
<td>(Least Privilege)</td>
<td>Supplemental guidance provided in control enhancement.</td>
<td>No</td>
</tr>
</tbody>
</table>
Mapping Vulnerabilities to Controls

<table>
<thead>
<tr>
<th>Control ID</th>
<th>Control Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCRM_AC-5</td>
<td>Separation Of Duties</td>
</tr>
<tr>
<td>SCRM_AC-6(1)</td>
<td>Least Privilege</td>
</tr>
<tr>
<td>SCRM_AC-11</td>
<td>Information Sharing</td>
</tr>
<tr>
<td>SCRM_AC-12</td>
<td>Publicly Accessible Content</td>
</tr>
<tr>
<td>SCRM_AU-3(1)</td>
<td>Audit Review, Analysis, And Reporting</td>
</tr>
<tr>
<td>SCRM_AU-4</td>
<td>Non-Repudiation</td>
</tr>
</tbody>
</table>

This table is Notional and does not represent any result.
### Mapping Controls to Standards, Practices and Regulation

<table>
<thead>
<tr>
<th>IDA Controls</th>
<th>Standards/Practices</th>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>DQA-QSLD</td>
<td>ISO9000</td>
<td>SAE/G19</td>
</tr>
<tr>
<td>DQA-QML</td>
<td>NISTIR-7622</td>
<td>AS6174</td>
</tr>
<tr>
<td>NQA-QPL</td>
<td>Open Group-O-TPPS</td>
<td>IDEA 1010</td>
</tr>
<tr>
<td>DQA-QPL</td>
<td>DMEA Trusted Suppliers</td>
<td>NDAA 818c</td>
</tr>
<tr>
<td>DQA-QPL</td>
<td>ISO/IEC 27036</td>
<td>Section 2319 of Title 10</td>
</tr>
<tr>
<td>DQA-QPL</td>
<td>SAE/G19, AS5533, AS6174</td>
<td>FAR Subpart 9.2</td>
</tr>
</tbody>
</table>

*This table is Notional and does not represent any result*
Next Steps

- **Trustworthy Suppliers Study**
  - Small working team is putting together a framework and first evaluation of what it means to be a “Trustworthy Supplier”
  - The result will give a broad view of the “Landscape”
  - This applies both to SCRM and Counterfeits
  - Next actions include
    - Involving a broader community to refine the work
    - Development of a toolbox
**REPORT DOCUMENTATION PAGE**

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

<table>
<thead>
<tr>
<th>1. REPORT DATE (DD-MM-YY)</th>
<th>2. REPORT TYPE</th>
<th>3. DATES COVERED (From – To)</th>
</tr>
</thead>
<tbody>
<tr>
<td>02-26-2015</td>
<td>Non-Standard DF</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th>5a. CONTRACT NUMBER</th>
<th>5b. GRANT NUMBER</th>
<th>5c. PROGRAM ELEMENT NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Framework for Understanding Trustworthy Suppliers</td>
<td>HQ0034-14-D-0001</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
<th>5d. PROJECT NUMBER</th>
<th>5e. TASK NUMBER</th>
<th>5f. WORK UNIT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian S. Cohen</td>
<td>DD-5-2635</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES</th>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute for Defense Analyses</td>
<td>NS D-5422</td>
</tr>
<tr>
<td>4850 Mark Center Drive</td>
<td>H 15-000085/1</td>
</tr>
<tr>
<td>Alexandria, VA 22311-1882</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
<th>10. SPONSOR’S / MONITOR’S ACRONYM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr. David Pentrack</td>
<td>DMEA</td>
</tr>
<tr>
<td>Defense Microelectronics Activity</td>
<td></td>
</tr>
<tr>
<td>4234 54th Street, McClellan, CA 95652-2100</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. DISTRIBUTION / AVAILABILITY STATEMENT</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>13. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Leader: Brian S. Cohen</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numerous practices and standards have been developed as a means of protecting against the possibility that counterfeit or altered components may be introduced into systems. This study develops a framework for viewing those practices and standards against a common set of criteria as a way of understanding how they are related and what they can achieve if applied.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15. SUBJECT TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeit, components, altered, standards, practices, framework</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. SECURITY CLASSIFICATION OF:</th>
<th>17. LIMITATION OF ABSTRACT</th>
<th>18. NUMBER OF PAGES</th>
<th>19a. NAME OF RESPONSIBLE PERSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. REPORT</td>
<td>Unlimited</td>
<td>14</td>
<td>Mr. David Pentrack</td>
</tr>
<tr>
<td>Unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. ABSTRACT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. THIS PAGE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unclassified</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19b. TELEPHONE NUMBER (Include Area Code)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(916) 231-1576</td>
</tr>
</tbody>
</table>
Appendix D: Attendees

John Adams, The Aerospace Corporation
Michael Adams, DLA Land & Maritime - VQC
Christopher Alberts, Software Engineering Institute
Brett Attaway, Synopsys, Inc.
Nicholas Avdellas, LMI Government Consulting
Jennifer Bisceglie, Interos Solutions, Inc.
Brent Bolner, NAVSEA 06L
Thomas Boydston, The Charles Stark Draper Laboratory, Inc.
Jon Boyens, National Institute of Standards and Technology
Theodore Bujewski, OSD/AT&L/Manufacturing and Industrial Policy
Chandra Caldwell, Air Force Office of Special Investigations
Dudley Caswell, IMTI-Integrated Manufacturing Technology Initiative
Mary Chung, Air Force Office of Special Investigations
Brian Cohen, Institute for Defense Analyses
Mark Cornwell, Decisive Analytics Corporation
Douglas Cummings, The Aerospace Corporation
Stephen D'Amour, Air Force Office of Special Investigations
Don Davidson, Trusted Mission Systems & Networks Office of the DoD CIO
Daniel Deisz, Rochester Electronics, LLC.
Karen Dixon-Brugh, Deputy Assistant Secretary of Defense (Systems Engineering)
Timothy Drumm, The Roosevelt Group
Glen Duke, National Security Agency
Jason Elder, Air Force Office of Special Investigations
Gerald Etzold, Aurora Semiconductor LLC
Tracee Gilbert, Engility
Jim Gobes, Intrinsix
Jason Gorey, Six O'Clock Ops, LLC.
Stewart Ocheltree, BAE Systems
Catherine Ortiz, Defined Business Solutions
Doug Palmer, Booz Allen Hamilton
Gregg Panning, Honeywell Corp
Andrew Parlock, Battelle
Sydney Pope, Deputy Assistant Secretary of Defense (Systems Engineering)
Jimmy Poplin, Defined Business Solutions
Paul Quirk, National Secure Manufacturing Center
Fred Schipp, Naval Surface Warfare Center Crane
Michael Scott, Jazz Semiconductor, Inc.
Joe Spruill, Lockheed Martin Corporation
Perry Tapp, Kansas City Plant
Peter Wheatley, Trusted Access Program Office
Melinda Woods, Department of Defense-OSD
Carol Woody, Software Engineering Institute
Edwin Yarbrough, Honeywell International
Ghassan Zamat, IBM Corporation