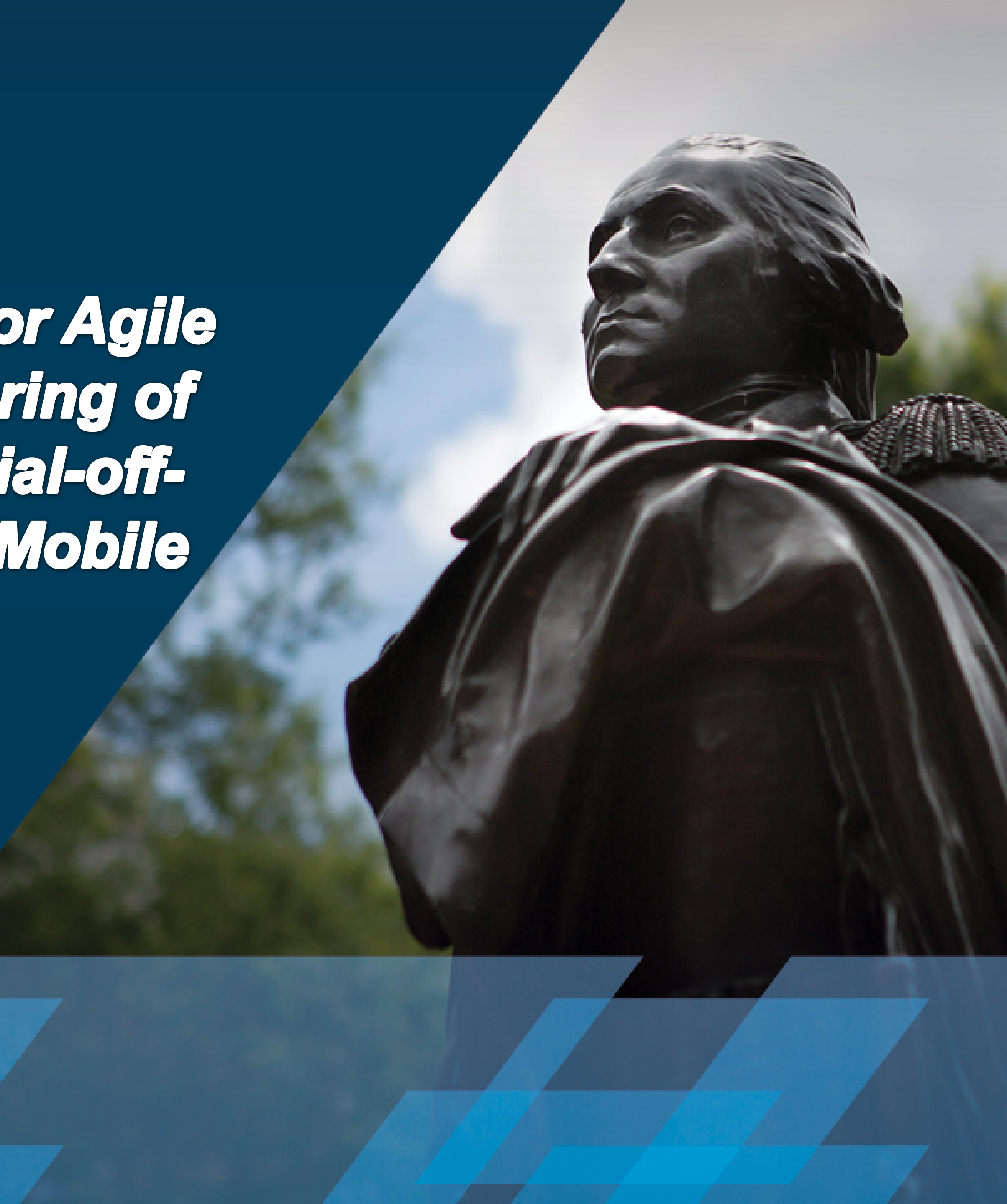
THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

An Architecture for Agile Systems Engineering of Secure Commercial-off-the-shelf (COTS) Mobile Communications

Jamieson Gump
Thomas Mazzuchi, D.Sc.
Shahram Sarkani, Ph.D., PE
George Washington University



Overview

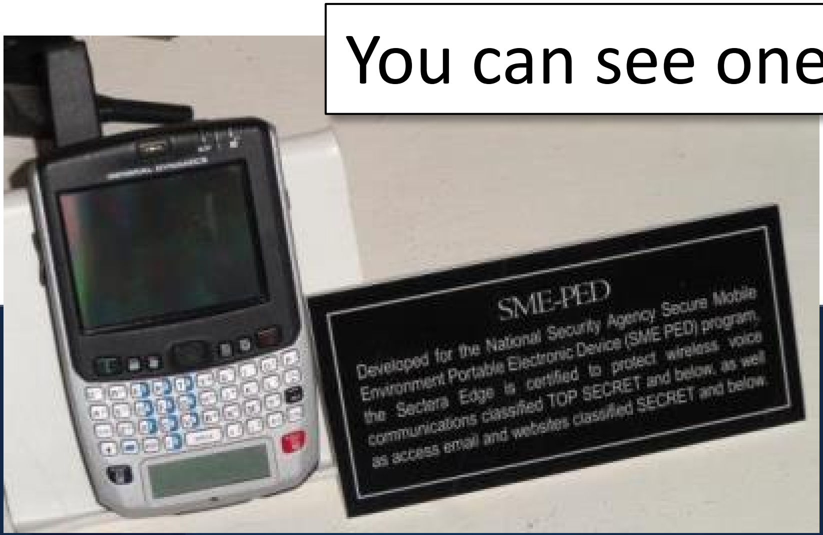
- Background
  - Legacy Solution
  - RMF, NIAP, Red/Black, CSfC
- COTS Integration
- Need for Architecture/Framework
- Overview of the Proposed Architecture
- Next Steps

“Cutting Edge” a Decade Ago

- Mobile Secure Communications needed by wide range of Government Users – expanding market
- Government (NSA) developed device took Years to develop … nearly obsolete when fielded
- Device is Controlled Cryptographic Item (CCI) – operator must ensure device is not lost
- NSA says - maybe industry can do better? – NSA can get partially out of the crypto business (for select applications)

https://www.nsa.gov/ia/news/2009/sme-ped.shtml

You can see one in the NSA Museum!



SME-PED

Developed for the National Security Agency Secure Mobile Environment Portable Electronic Device (SME PED) program, the Sectera Edge is certified to protect wireless voice communications classified TOP SECRET and below, as well as access email and websites classified SECRET and below.

Risk Management Framework (RMF)

Risk Management Framework (RMF) for DoD Information Technology (IT)

DODI 8510.01, March 12, 2014, DoD CIO

“The cybersecurity requirements for DoD information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 …”

NIST Special Publication 800-37
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

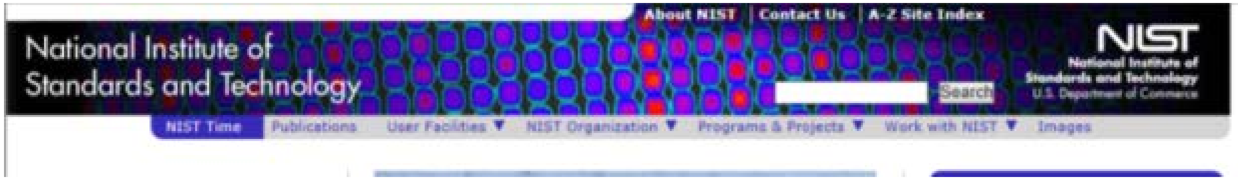
INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director



National Institute of Standards and Technology

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

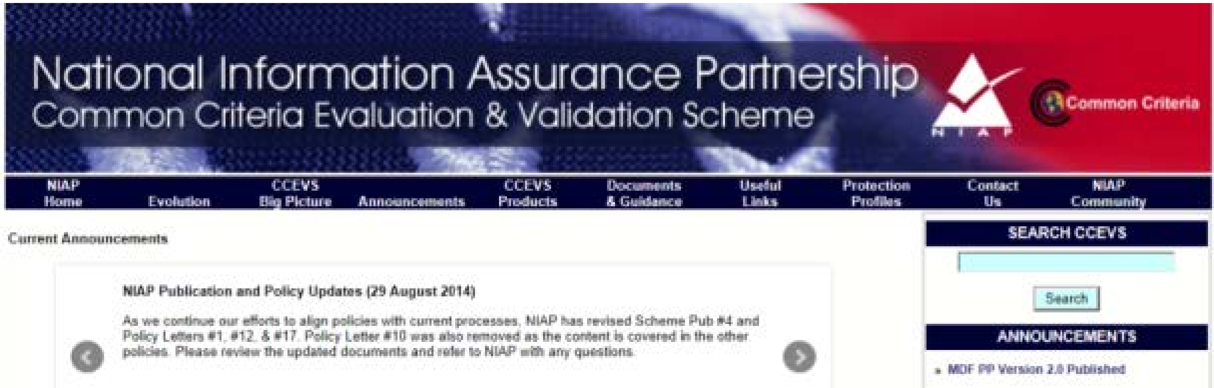
http://www.nist.gov/

National Information Assurance Partnership (NIAP)

“The focus of the NIAP is to establish a national program for the evaluation of information technology products for conformance to the International Common Criteria for Information Technology Security Evaluation. …

The NIAP maintains a Product Compliance List (PCL) containing all IT products and protection profiles that have successfully completed evaluation and validation under the scheme.”

https://www.niap-ccevs.org/



Current Announcements

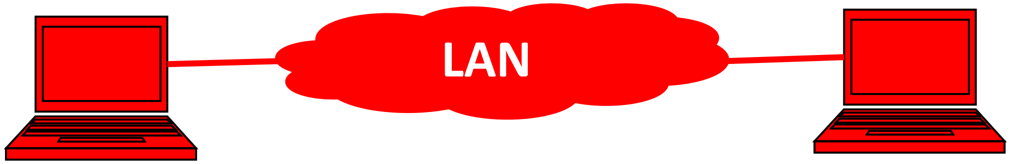
NIAP Publication and Policy Updates (29 August 2014)

As we continue our efforts to align policies with current processes, NIAP has revised Scheme Pub #4 and Policy Letters #1, #12, & #17. Policy Letter #10 was also removed as the content is covered in the other policies. Please review the updated documents and refer to NIAP with any questions.

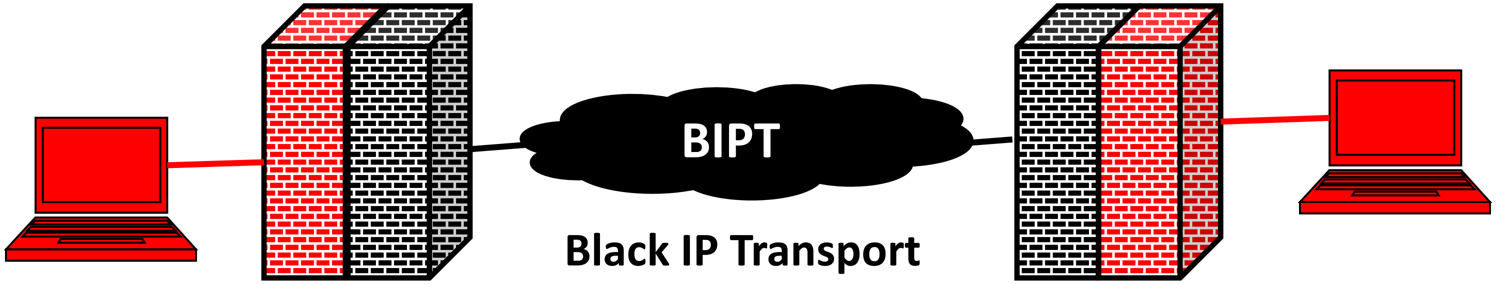
- MDF PP Version 2.0 Published

Red/Black Introduction

- Red (Plain Text) and Black (Cypher Text)
- For environments where the communications are “protected”



- For communications where the transport can not be “protected”

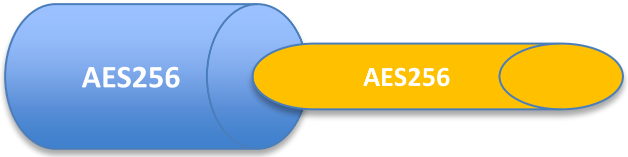


Commercial Solutions for Classified (CSfC)

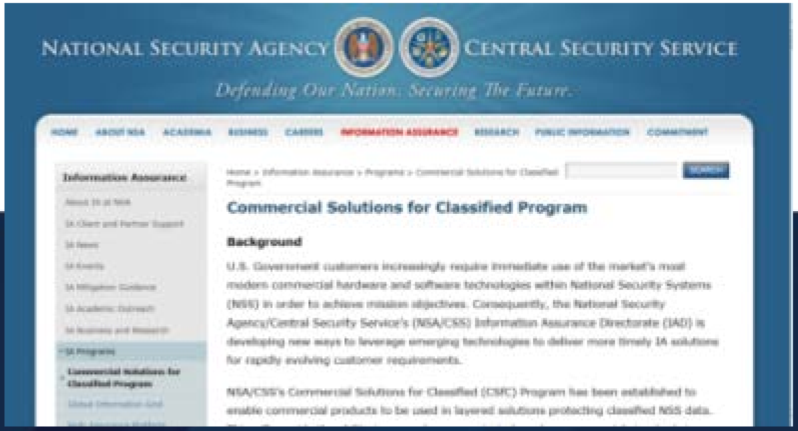
Foundation is the Commercial Solutions for Classified (CSfC) program

https://www.nsa.gov/ia/programs/csfc_program/

Public information – "This will provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years."



Example - VPN Tunnel Inside another tunnel



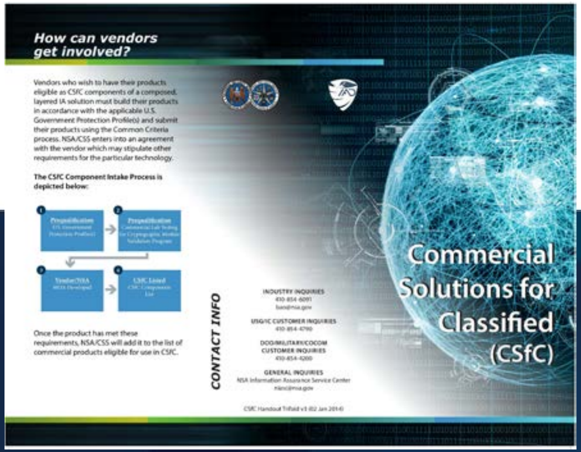
Home > Information Assurance > Programs > Commercial Solutions for Classified Program

Commercial Solutions for Classified Program

Background

U.S. Government customers increasingly require immediate use of the market's most modern commercial hardware and software technologies within National Security Systems (NSS) in order to achieve mission objectives. Consequently, the National Security Agency/Central Security Service's (NSA/CSS) Information Assurance Directorate (IAD) is developing new ways to leverage emerging technologies to deliver more timely IA solutions for rapidly evolving customer requirements.

NSA/CSS's Commercial Solutions for Classified (CSfC) Program has been established to enable commercial products to be used in layered solutions protecting classified NSS data.


Prequalification
U.S. Government Protection Profile(s)
Prequalification
Commercial Lab Testing for Cryptographic Module Validation Program
Vendor/NSA
MOA Developed
CSfC Listed
CSfC Components List
Commercial Solutions for Classified (CSfC)

How can vendors get involved?

Vendors who wish to have their products eligible as CSfC components of a composed, layered IA solution must build their products in accordance with the applicable U.S. Government Protection Profile(s) and submit their products using the Common Criteria process. NSA/CSS enters into an agreement with the vendor which may stipulate other requirements for the particular technology.

The CSfC Component Intake Process is depicted below:

Once the product has met these requirements, NSA/CSS will add it to the list of commercial products eligible for use in CSfC.

CONTACT INFO

INDUSTRY INQUIRIES
410-854-6091
[illegible]@nsa.gov

USG/IC CUSTOMER INQUIRIES
410-854-4790

DOD/MILITARY/COCOM
CUSTOMER INQUIRIES
410-854-4200

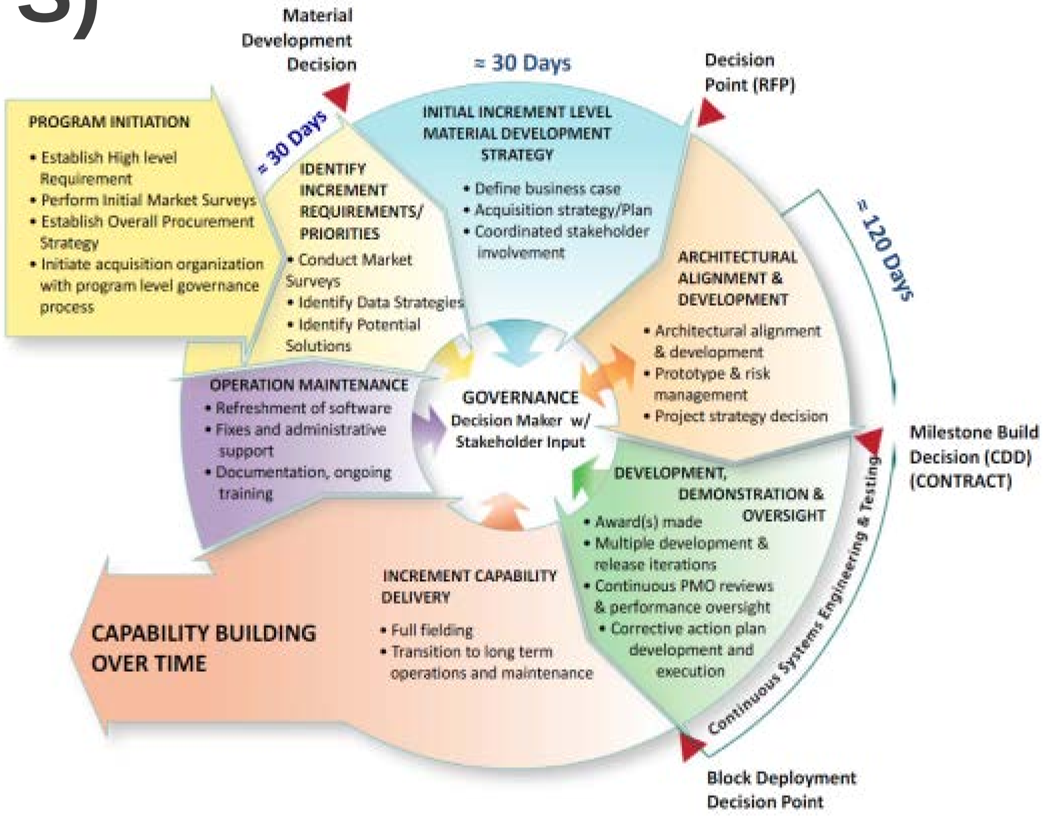
GENERAL INQUIRIES
NSA Information Assurance Service Center
niasc@nsa.gov

CSfC Handout Trifold v1 (02 Jan 2014)

IT Acquisition Processes Can Be Applied (integration of COTS)

Architecture is the product/integration of:

- **Secure Mobile COTS (CSfC)**
- **Evaluation by vendors during development (NIAP/CC)**
- **Integration methods to rapidly integrate (IT360)**
- **Field and iterate ….**



Material Development Decision

≈ 30 Days

Decision Point (RFP)

≈ 30 Days

PROGRAM INITIATION

- Establish High level Requirement
- Perform Initial Market Surveys
- Establish Overall Procurement Strategy
- Initiate acquisition organization with program level governance process

IDENTIFY INCREMENT REQUIREMENTS/ PRIORITIES

- Conduct Market Surveys
- Identify Data Strategies
- Identify Potential Solutions

INITIAL INCREMENT LEVEL MATERIAL DEVELOPMENT STRATEGY

- Define business case
- Acquisition strategy/Plan
- Coordinated stakeholder involvement

≈ 120 Days

ARCHITECTURAL ALIGNMENT & DEVELOPMENT

- Architectural alignment & development
- Prototype & risk management
- Project strategy decision

GOVERNANCE

Decision Maker w/ Stakeholder Input

OPERATION MAINTENANCE

- Refreshment of software
- Fixes and administrative support
- Documentation, ongoing training

Milestone Build Decision (CDD) (CONTRACT)

DEVELOPMENT, DEMONSTRATION & OVERSIGHT

- Award(s) made
- Multiple development & release iterations
- Continuous PMO reviews & performance oversight
- Corrective action plan development and execution

INCREMENT CAPABILITY DELIVERY

- Full fielding
- Transition to long term operations and maintenance

CAPABILITY BUILDING OVER TIME

Continuous Systems Engineering & Testing

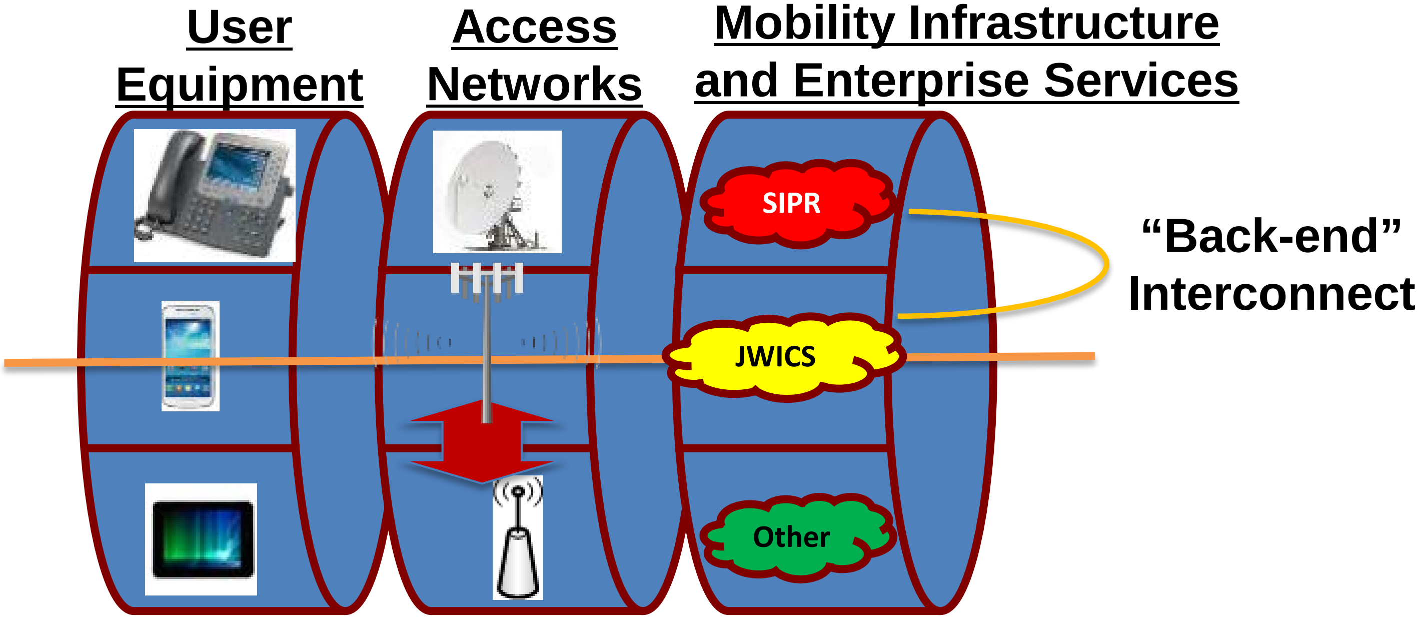
Block Deployment Decision Point

IT Acquisition: Expediting the Process to Deliver Business Capabilities to the DoD Enterprise (Jul 2012)

Need for Architecture/Framework

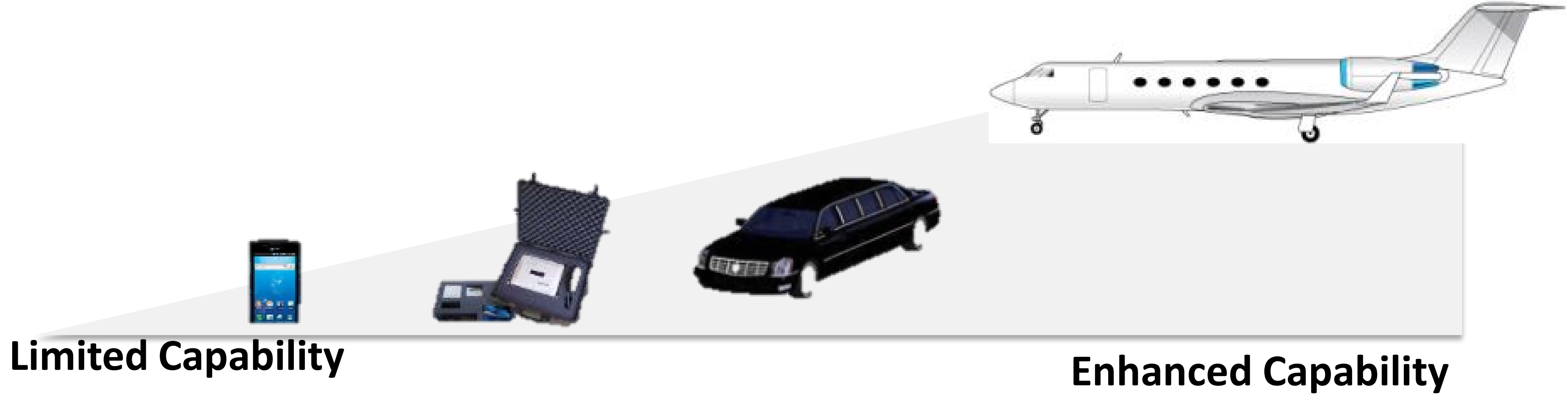
- To improve interoperability and to ensure efficiencies in composed solutions an “overarching” architecture is required
- Government has provided direction and guidance, but no secure mobile architecture exists
- With the increasing use of commercial technology techniques are needed to support rapid integration
- With rapidly evolving mobile technology and the exponential increase in products coupled with the emerging security solutions this architecture is critical for the community

“Combination Lock” Architecture



1. Compose solution by “turning the dials”
2. Device “provisioned” (configured) for specific enterprise
3. Transport can be changed during operation of the device (user can move from cellular to WIFI, etc)
4. Transport can be shared by multiple devices

Broad Range of User Equipment can be Supported by this Technology



- User Devices Paired with Access Networks (Transport) based on Operational Needs
- Owner/Operator of device reaches back to their respective enterprise services

Access Networks

- PSTN

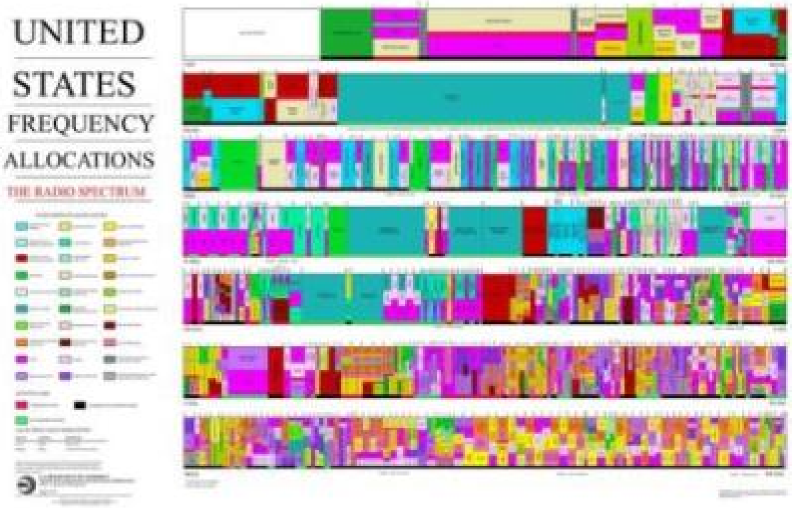
- Cellular

- Fiber Optic

- WIFI

- RF (LMR/SATCOM), etc

- Combination of Above
- May include “Smooth” Transition from one to another



Black (Cypher Text) Transport

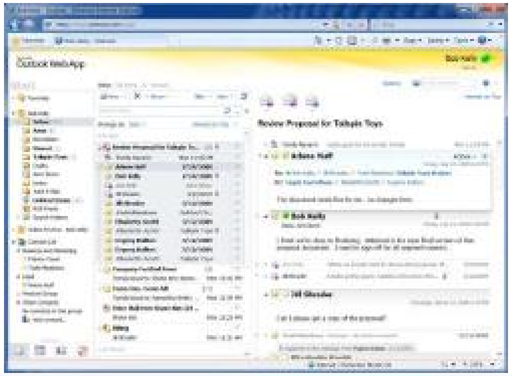
Mobility Infrastructure and Enterprise Services

- Mobility Infrastructure terminates the secure connection from the mobile device – “Landing Zone”
- Full range of Enterprise Services can be supported – Voice, Video, and Data
- Services built on commercial technology – mission specific web sites can augment email

Voice

Video

Data



Next Steps

- Expand on the secure communications architecture
  - Focus on identity management and end-to-end security
  - Include support for standardized campus WIFI solutions using “best practices”
  - Incorporate latest commercial technologies
- Follow on-going development of NSA Capability Packages
- Develop an “executable” architecture (simulation) to support the development alternatives analysis and model potential solutions
- Engage with active community - a “dozen” solutions coming on line this winter

Questions & Comments?

17th Annual Systems Engineering Conference

OCTOBER 27-30, 2014

WWW.NDIA.ORG/MEETINGS/5870

“An Architecture for Agile Systems Engineering of Secure Commercial-off-the-shelf (COTS) Mobile Communications”

Jamieson Gump

Thomas Mazzuchi, D.Sc. Shahram Sarkani, Ph.D., PE

George Washington University

Presenter Biography

JAMIESON GUMP

Jim Gump is a Ph.D. candidate at George Washington University in the Engineering Management and Systems Engineering curriculum. As the assistant program area manager for the national command programs area at the Johns Hopkins University Applied Physics Laboratory, he assists the DOD CIO office which provides assured, continuous senior leader and interagency communications to the National Leadership Command community. He has a B.S. in electrical engineering from the University of Vermont, an M.S. in engineering management from Western New England College. He has more than 30 years of experience as a senior systems engineer and has co-founded, Paradigm Technologies Inc, a successful engineering firm providing engineering services to the DOD. He is also an experienced military intelligence officer having served for 20 years in the U. S. Army Reserves.

978-512-9665 (cell)
Jim.Gump@jhuapl.edu

Presenter Biography

THOMAS MAZZUCHI, D.Sc.,

THOMAS MAZZUCHI, D.Sc., is Chair and Professor at the School of Engineering Management and Systems Engineering (EMSE) at The George Washington University where he also previously served as the Chair of the Operations Research Department and as Interim Dean of the School of Engineering and Applied Science. Dr. Mazzuchi has been engaged in consulting and research in the area of reliability, risk analysis, and quality control for over twenty years. He served as a research mathematician with the Royal Dutch Shell Company, has held research contracts with numerous state and government agencies including NASA, the U.S. Army, the U.S. Air Force and the U.S. Postal Service.

Presenter Biography

SHAHRAM SARKANI, Ph.D., P.E.,

SHAHRAM SARKANI, Ph.D., P.E., is Professor of Engineering Management and Systems Engineering (EMSE) at The George Washington University. Since joining the faculty in 1986, he has served as a Department Chair and Interim Associate Dean and was appointed as Faculty Adviser and Academic Director of EMSE Off-Campus Programs in 2001. In his current role, Professor Sarkani designs and administers off campus MS and programs at over 20 locations world-wide that serve more than 1,000 students. As author of over 150 technical publications and presentations, he remains engaged with important ongoing research in the field of systems engineering.

SHAHRAM SARKANI, Ph.D., P.E., is Professor of Engineering Management and Systems Engineering (EMSE) at The George Washington University. Since joining the faculty in 1986, he has served as a Department Chair and Interim Associate Dean and was appointed as Faculty Adviser and Academic Director of EMSE Off-Campus Programs in 2001. In his current role, Professor Sarkani designs and administers off campus MS and programs at over 20 locations world-wide that serve more than 1,000 students. As author of over 150 technical publications and presentations, he remains engaged with important ongoing research in the field of systems engineering.

Abstract

The federal Government has long had a need for secure communications. The National Security Agency (NSA) is responsible for the wide range of technologies to secure these communications. They have realized, recently, that the development times for Government encryption technology was not keeping pace with the rapid evolution of commercial mobile technologies coupled with a realization that commercial technologies exist to meet the requirements for the federal Government. Specifically, NSA has published specifications on their website to operationalize these capabilities. Commercial Solutions for Classified (CSfC), NSA term for COTS secure communications, coupled with published capability packages allows a developer to rapidly field a secure communications solution built entirely on Commercial off the Shelf (COTS) technology. This allows for rapid fielding of the capabilities for a wide range of applications. The end user is presented with the latest in mobile communications technologies with the software security applied after market. The first users of this technology are within the Department of Defense (DoD); other agencies are anticipated to field capabilities as well. No architecture exists to aid in the development of these capabilities and research is required to develop an overarching architecture to support these emerging capabilities. This architecture will address the rapidly evolving commercial mobile security market and address fully leveraging commercial technologies to field the latest technologies in the shortest amount of time and at the lowest cost. With the encryption built on software (vice hardware) Agile Engineering techniques can be readily applied. Although developed in the US for the federal Government this approach has been adopted by other governments and is anticipated to be adopted by commercial users for enhanced security. With the NSA move to commercial technologies and the commercial market moving to enhanced security for “standard commercial users” there is an emerging convergence of these two approaches. An architectural construct to support this growing user base is the focus of this research. The method to be employed is to survey the wide range of implementations currently being fielded using a case study methodology, developing an effective overarching architectural contract and returning to the Subject Matter Experts (SMEs) across this community to validate the architecture. The utility of the architecture will be rooted in the ability to aid the full range of customers; from mobile phone solutions, to secure laptops and fixed communications at remote sites. The initial work has revealed effective architectural constructs to support the wide range of emerging applications of this promising approach from NSA – commercial solutions for classified.

References

Government Sites mentioned on prior charts, plus …

Journal Papers (highlights from research)

- **The National Security Agency (NSA) wrote 3 critical papers this year that directly contribute to this effort:**
  - Plunkett, D. A. (2014). Achieving Confidence in Cyberspace in an Ever-Changing Ecosystem. *Journal of Information Warfare*, *13*, 1-7
  - Boyle, M. (2014). Information Assurance Standards: A Cornerstone for Cyber Defense. *Journal of Information Warfare*, *13*, 8-18.
  - Watkins, J. (2014). Outmaneuvering Cyber Adversaries Using Commercial Technologies. *Journal of Information Warfare*, *13*, 76-86.
- **Identity management critical component**
  - Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., & Germonville, D. (2014). Adding Federated Identity Management to OpenStack. Journal of Grid Computing, 12(1), 3-27.
- **COTS Integration Process** - Rosa, W., Packard, T., Krupanand, A., Bilbro, J. W., & Hodal, M. M. (2013). COTS integration and estimation for ERP. *Journal of Systems and Software*, *86*(2), 538-550.
- **NIAP and Protection Profiles** - Alves-Foss, J., Taylor, C., & Oman, P. (2004, January). A multi-layered approach to security in high assurance systems. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on* (pp. 10-pp). IEEE.

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC