Davidson Technologies:

A Medium Sized Business Experience with DFARS 7012/NIST 800-171

Davidson Technologies

Missiles • Aerospace • Cyber • Intelligence

Davidson Technologies

- Founded in 1996 by Dr. Julian Davidson
- “Father of Missile Defense in America” – Sen. Jeff Sessions
- After Dr. Julian Davidson death in 2013 Dr. Dorothy Davidson stepped in to run the company as a woman-owned small business
- Our Capabilities:

Missiles

Aerospace

Cyber

Intelligence

- 2016 Nunn-Perry Award winner with Northrop Grumman on the Mentor-Protégé Program

Davidson Technologies - A New Cyber System?

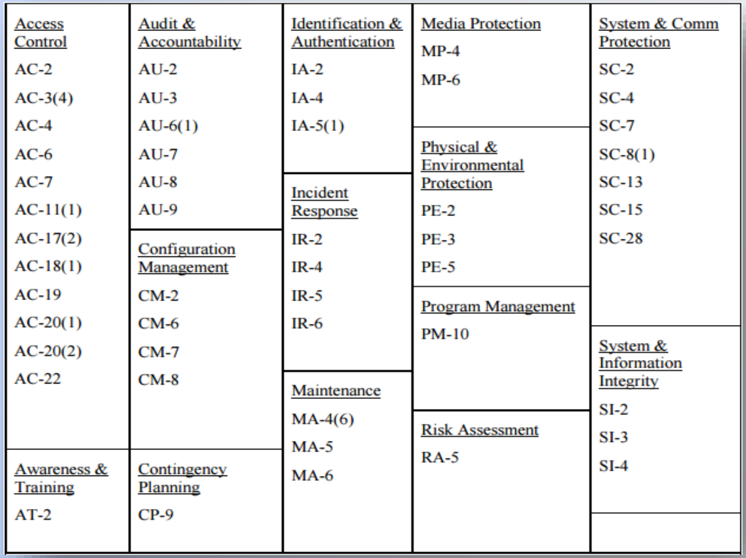
Cyber is a core capability, so how does DTI's internal cyber stack up?

If it ain't broke…

Davidson Technologies
Missiles • Aerospace • Cyber • Intelligence

Davidson Technologies - Cyber Driver

"The Department [DoD] is now realizing that there is a plethora of data that is not classified, but that can provide potential adversaries with a wealth of information about our operations and systems." – Mr. Lee Rosenberg, Director MDA OSBP from OSBP Quarterly Newsletter | January 2016



Access Control AC-2 AC-3(4) AC-4 AC-6 AC-7 AC-11(1) AC-17(2) AC-18(1) AC-19 AC-20(1) AC-20(2) AC-22	Audit & Accountability AU-2 AU-3 AU-6(1) AU-7 AU-8 AU-9	Identification & Authentication IA-2 IA-4 IA-5(1)	Media Protection MP-4 MP-6	System & Comm Protection SC-2 SC-4 SC-7 SC-8(1) SC-13 SC-15 SC-28
Awareness & Training AT-2	Configuration Management CM-2 CM-6 CM-7 CM-8	Incident Response IR-2 IR-4 IR-5 IR-6	Physical & Environmental Protection PE-2 PE-3 PE-5	System & Information Integrity SI-2 SI-3 SI-4
	Contingency Planning CP-9	Maintenance MA-4(6) MA-5 MA-6	Program Management PM-10	
			Risk Assessment RA-5	

- **51 NIST 800-53 Controls**
  - AC: Access Control
  - AT: Awareness Training
  - AU: Auditing and Accountability
  - CM: Configuration Management
  - CP: Contingency Planning
  - IA: Identification and Authentication
  - IR: Incident Response
  - …

Davidson Technologies - New Cyber System

The Primary Goals

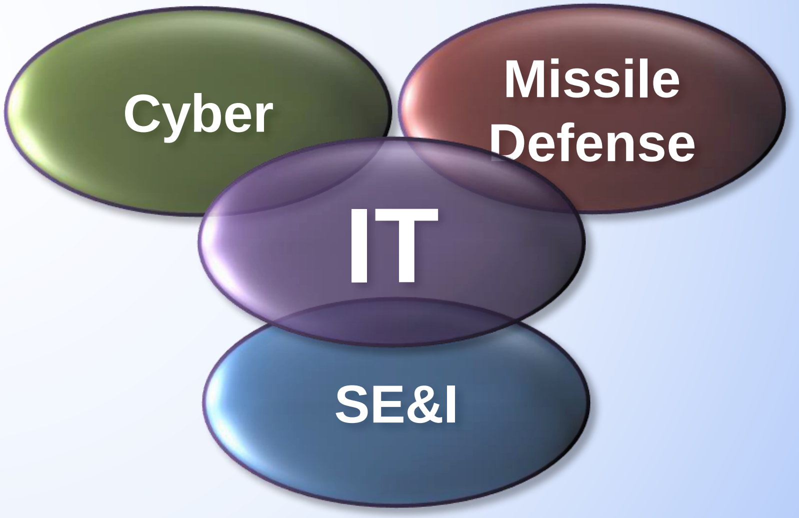
- Provide a secure computing environment to meet or exceed all regulatory compliance requirements
- Allow for easy and seamless access to data and processing capabilities for all employees
- Ensure data integrity and confidentiality by bringing the users to the data, instead of sending the data to the users
- Maintain modularity for easy and affordable scalability
- Operate on a minimal footprint, both environmentally and operationally

ACSIS - Automated Cyber Secure Information System

ACSIS is a secure virtualized cyber framework enabling end users access to network resources from anywhere with any device while maintaining regulatory compliance

- An investment by Davidson Technologies to design a multi-purpose/multi-application system capable of meeting high end processing, big data, and regulatory compliance

- Designed and implemented by DTI Cyber/IT professionals with core competencies in systems and cyber engineering with DoD and other regulatory domain knowledge



Davidson Technologies
Missiles • Aerospace • Cyber • Intelligence

ACSIS - Certified Engineers and Architects

PMI®
PMP®

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

C|EH™
Certified Ethical Hacker

ITIL®

GIAC
GLOBAL INFORMATION ASSURANCE CERTIFICATION
www.giac.org

CGEIT®
Certified in the Governance of Enterprise IT®
An ISACA® Certification

CISA®
Certified Information Systems Auditor®
An ISACA® Certification

CISM®
Certified Information Security Manager®
An ISACA® Certification

CRISC™
Certified in Risk and Information Systems Control™
An ISACA® Certification

Microsoft
CERTIFIED
Solutions Expert
Messaging

Microsoft®
CERTIFIED
Systems Administrator

Microsoft®
CERTIFIED
Systems Engineer

vmware®
CERTIFIED
PROFESSIONAL
DATA CENTER VIRTUALIZATION

solaris
Sun microsystems
CERTIFIED
System Administrator

redhat.
CERTIFIED SYSTEM ADMINISTRATOR

CISCO CERTIFIED
CCNA

CISCO CERTIFIED
CCNP

CISCO CERTIFIED
CCDA

CISCO CERTIFIED
CCDP
DESIGN

CompTIA
Security+™
CERTIFIED

CompTIA
Server+®
CERTIFIED

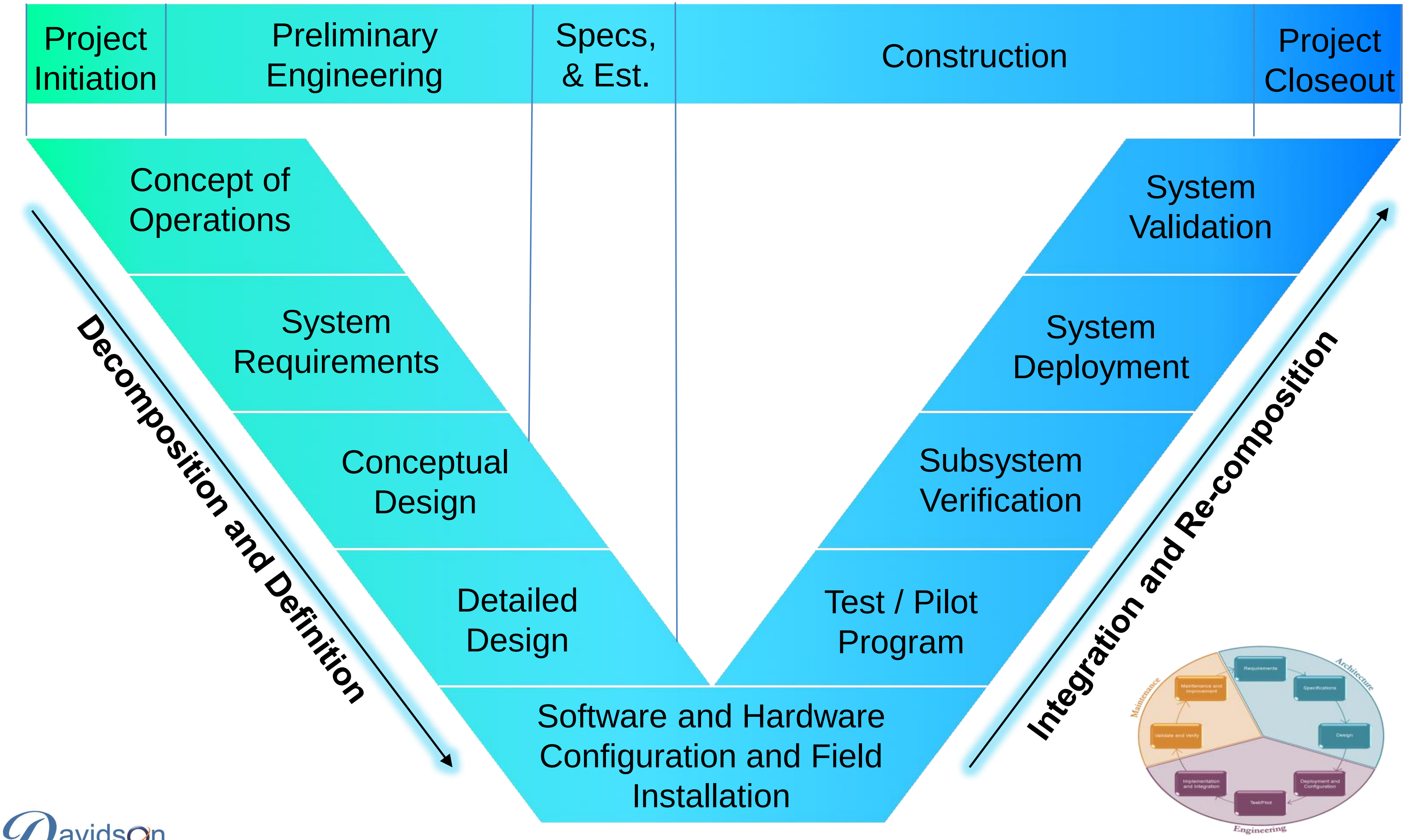
CompTIA
Network+®
CERTIFIED

CompTIA
A+®
CERTIFIED
ce

CompTIA
Project+™
CERTIFIED

CompTIA
Linux+

ACSIS - Traditional Engineering Drove Design and Documentation



Project Initiation

Preliminary Engineering

Specs, & Est.

Construction

Project Closeout

Concept of Operations

System Requirements

Conceptual Design

Detailed Design

Software and Hardware Configuration and Field Installation

Test / Pilot Program

Subsystem Verification

System Deployment

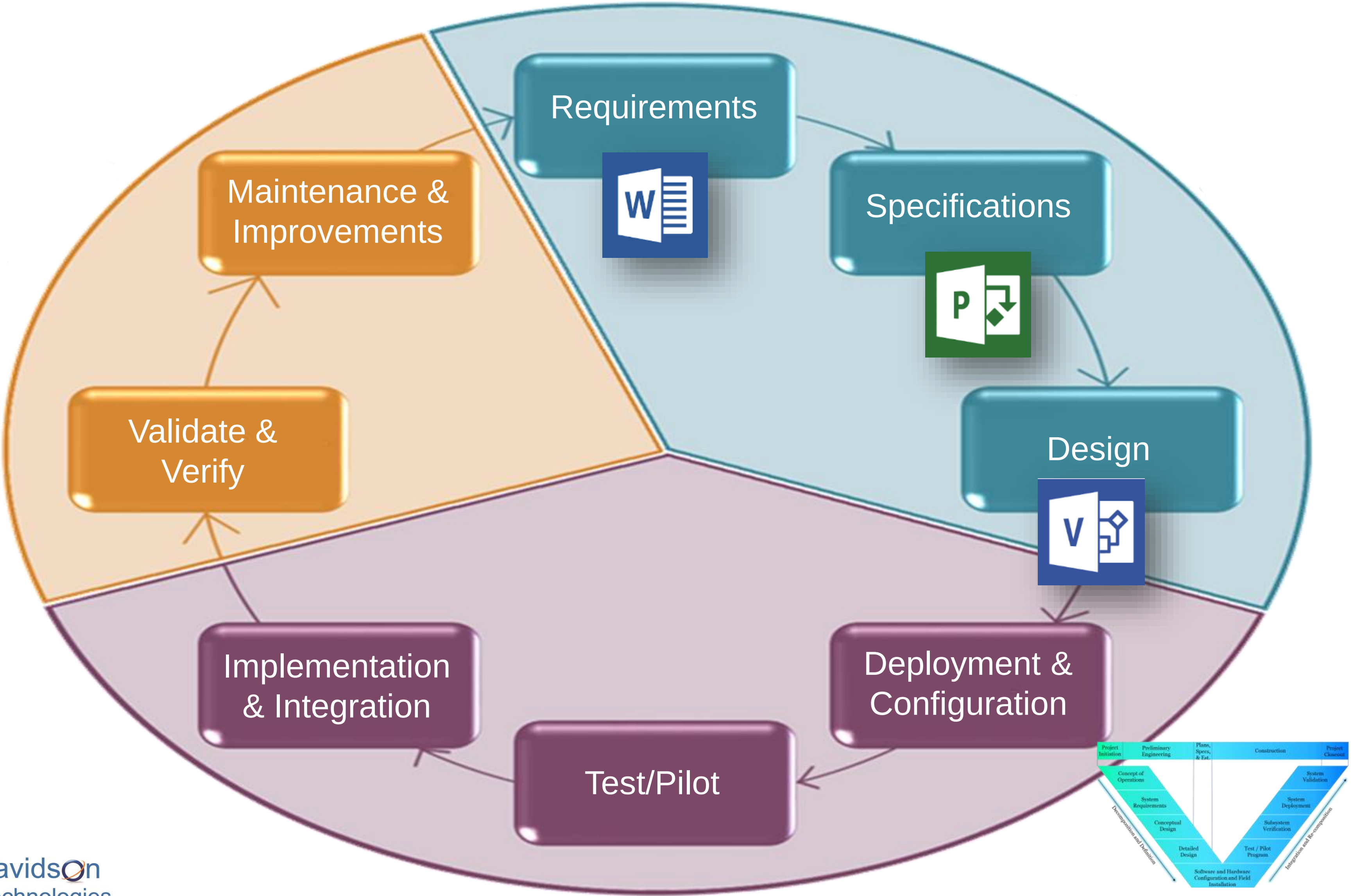
System Validation

Decomposition and Definition

Integration and Re-composition

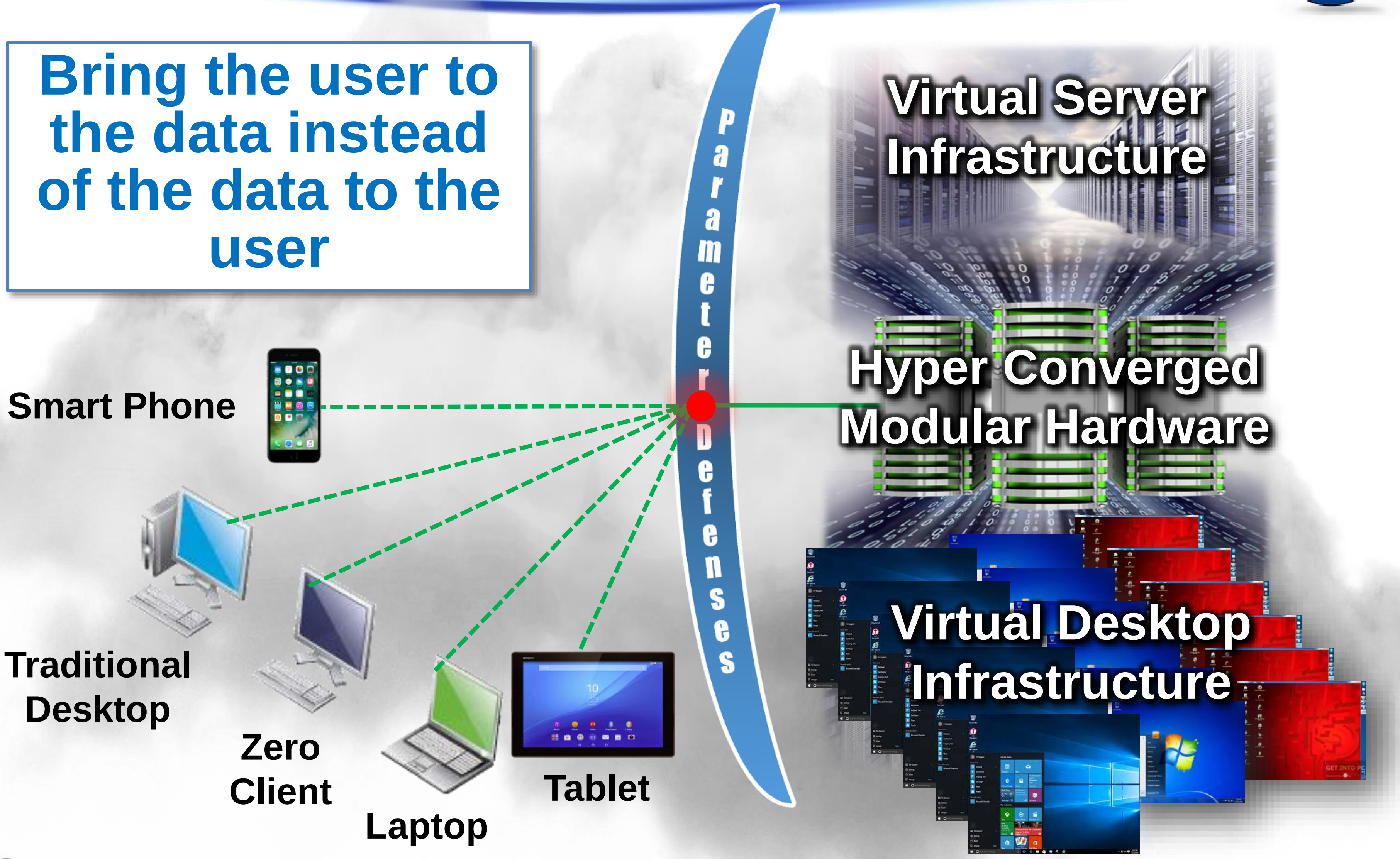
Davidson Technologies
Missiles • Aerospace • Cyber • Intelligence

ACSIS - Continuous Life Cycle Development



ACSIS - Architecture

Bring the user to the data instead of the data to the user



Smart Phone

Traditional Desktop

Zero Client

Laptop

Tablet

Parameter Defenses

Virtual Server Infrastructure

Hyper Converged Modular Hardware

Virtual Desktop Infrastructure

ACSIS - Why VDI? (PROs Vs. CONs)

PROs

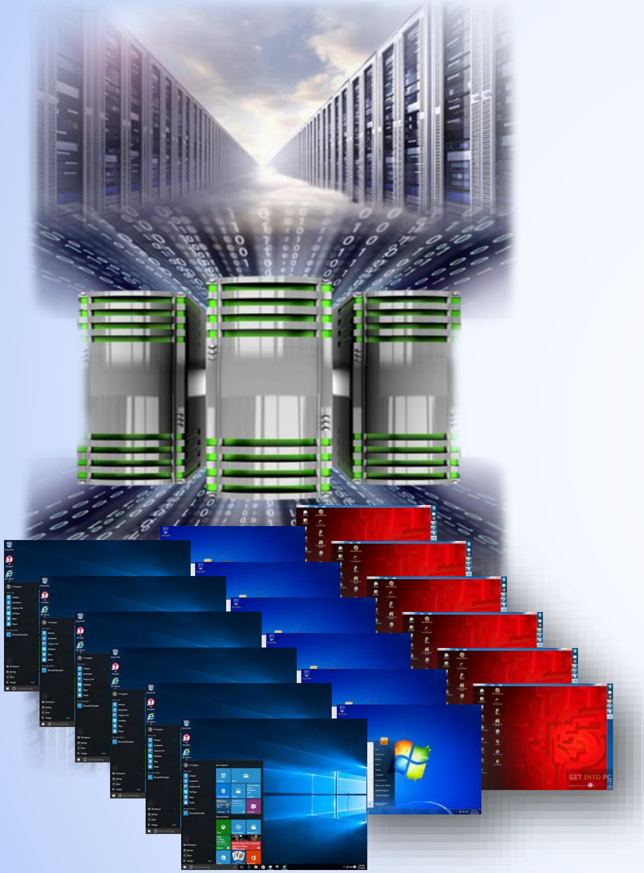
- Data Protection
- Desktop Configuration Control
- Vulnerability Management
- Patch Management
- License Management
- Virtual Application Delivery
- Easy Resource Allocation
- Continuous User Experience
- Access from Secure Locations
- Easy Remote Access
- ROI for End Point Devices
- Revitalization of IT assets
- Centralized Desktop Support
- BYOD Policy Enforcement

CONs

- Eggs all in one basket
- Physical Security
- Bandwidth and Storage
- IT becomes 24/7 (no network = no infrastructure)
- Subject Matter Experts
- TDY with no network

Virtual Desktop Infrastructure

ACSIS - Lessons Learned



- Maintain Interoperability Chart for all Virtualization Vendors' Software and Versions.
- Provide users an opportunity to learn and understand VDI
- Be careful of the bleeding edge… It can hurt
- Continue to evaluate new products
- Invest in the appropriate monitoring tools and dashboards

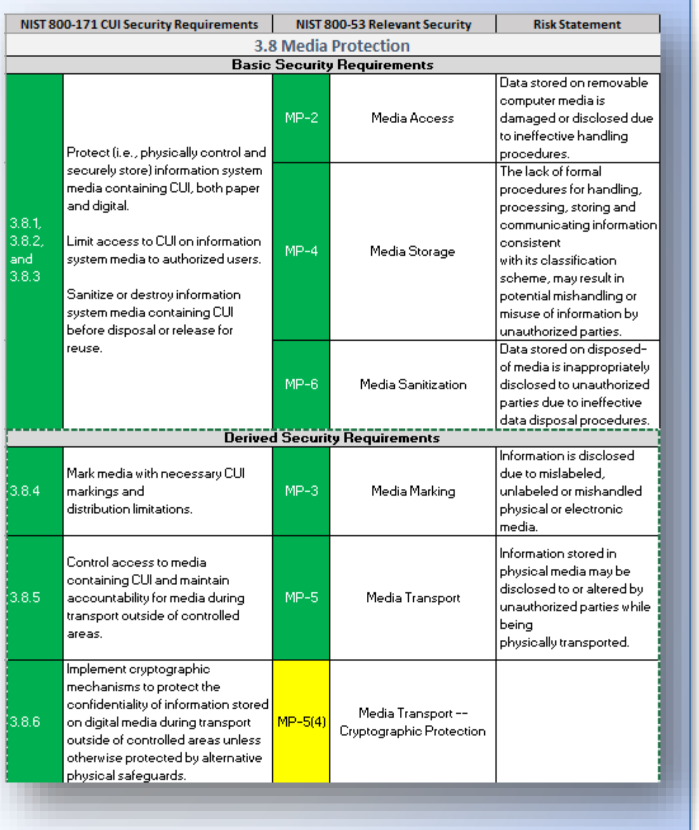
Why ACSIS?

- Economical and Modular for Easy Scalability
- Centralized Management and Configuration
- Layered Security (Security In-Depth)
- Ease of Access and Usability
- Minimal Footprint

Davidson Technologies
Missiles • Aerospace • Cyber • Intelligence

ACSIS - Recurring Questions & Enduring Issues

- **Is it CUI or UCTI or CDI or…?**
- **What is considered CUI/UCTI/CDI…?**
- **Do we have CUI/UCTI/CDI?**
- **Who is certifying / accrediting that systems are compliant?**

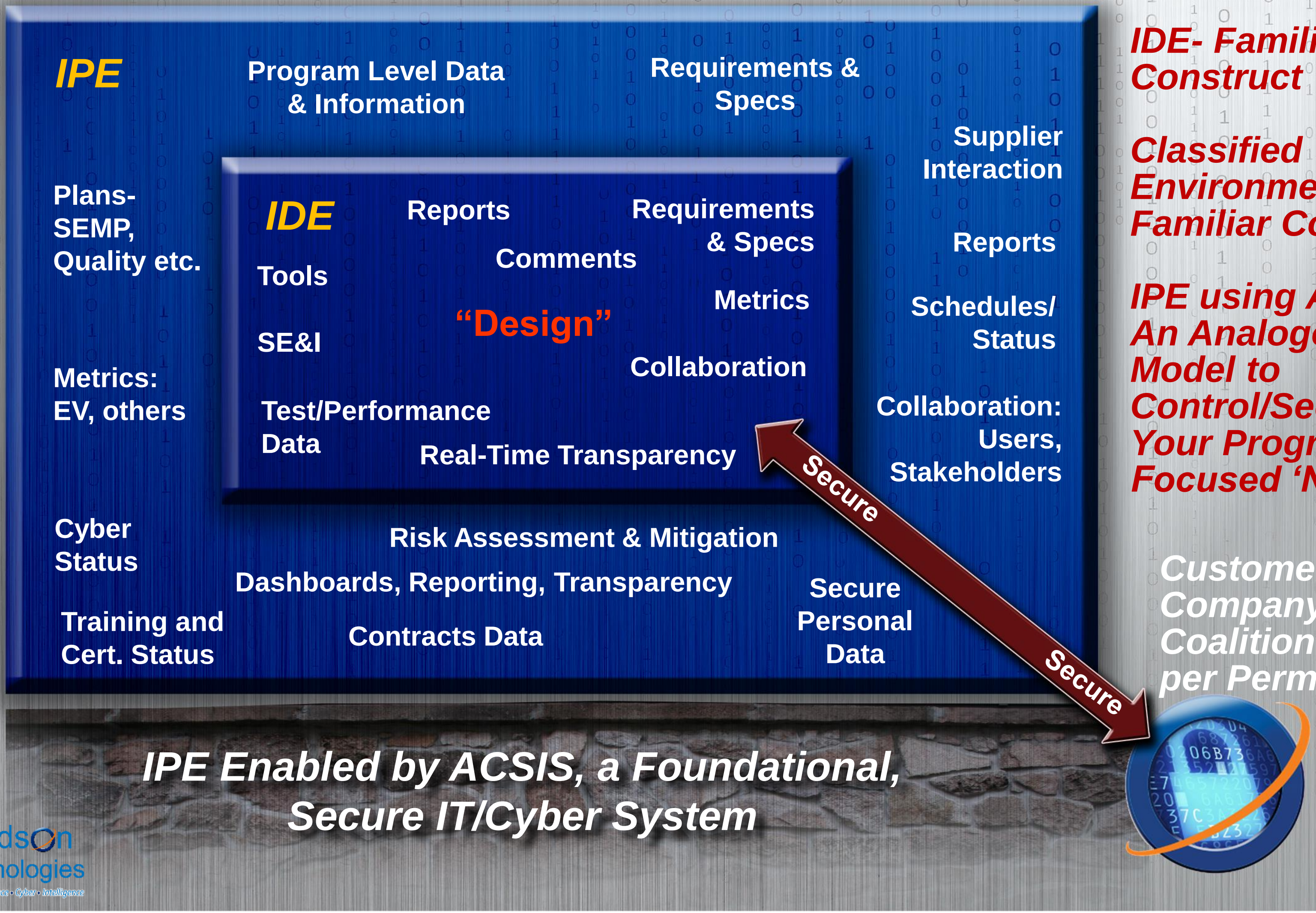


NIST 800-171 CUI Security Requirements		NIST 800-53 Relevant Security		Risk Statement
3.8 Media Protection				
Basic Security Requirements				
3.8.1, 3.8.2, and 3.8.3	Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital. Limit access to CUI on information system media to authorized users. Sanitize or destroy information system media containing CUI before disposal or release for reuse.	MP-2	Media Access	Data stored on removable computer media is damaged or disclosed due to ineffective handling procedures.
		MP-4	Media Storage	The lack of formal procedures for handling, processing, storing and communicating information consistent with its classification scheme, may result in potential mishandling or misuse of information by unauthorized parties.
		MP-6	Media Sanitization	Data stored on disposed-of media is inappropriately disclosed to unauthorized parties due to ineffective data disposal procedures.
Derived Security Requirements				
3.8.4	Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	Information is disclosed due to mislabeled, unlabeled or mishandled physical or electronic media.
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	Information stored in physical media may be disclosed to or altered by unauthorized parties while being physically transported.
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of information stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	MP-5(4)	Media Transport -- Cryptographic Protection	

- **Will our self NIST 800-171 assessment suffice?**

Secure Cyber Supply Chain

Offering Suppliers an Integrated Program Environment (IPE)



IPE

Program Level Data & Information

Requirements & Specs

Supplier Interaction

Plans-SEMP, Quality etc.

IDE

Reports

Requirements & Specs

Comments

Tools

Metrics

“Design”

SE&I

Collaboration

Test/Performance Data

Real-Time Transparency

Reports

Schedules/ Status

Collaboration: Users, Stakeholders

Metrics: EV, others

Cyber Status

Risk Assessment & Mitigation

Dashboards, Reporting, Transparency

Secure Personal Data

Training and Cert. Status

Contracts Data

IPE Enabled by ACSIS, a Foundational, Secure IT/Cyber System

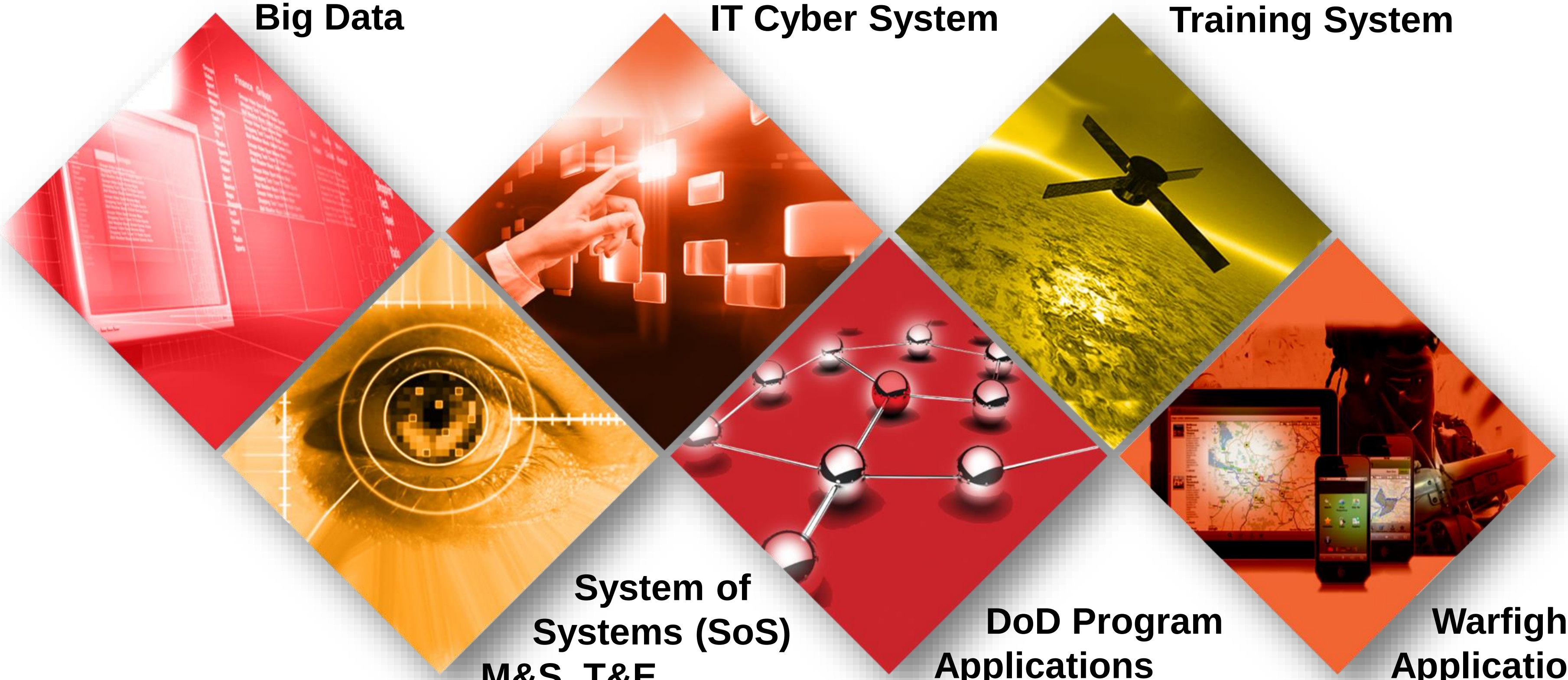
IDE- Familiar Construct

Classified Environment- Familiar Construct

IPE using ACSIS- An Analogous Model to Control/Secure Your Program- Focused ‘Network’

Customer, Company, Team, Coalition Users per Permissions

ACSIS Potential Applications



Big Data

IT Cyber System

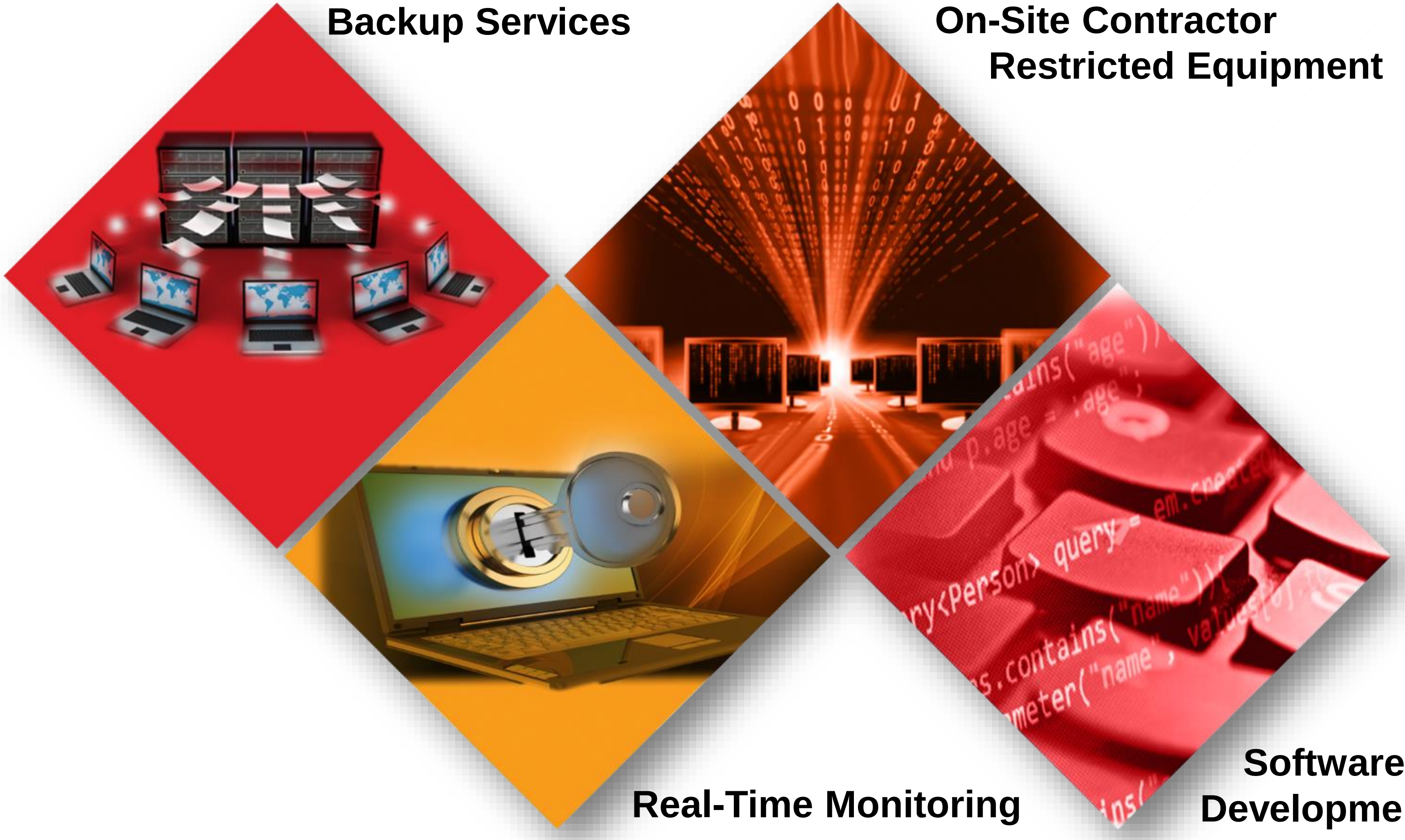
Training System

System of Systems (SoS) M&S, T&E

DoD Program Applications

Warfighter Applications

ACSIS Potential Applications



Backup Services

On-Site Contractor
Restricted Equipment

Real-Time Monitoring

Software
Development Lab

ACSIS

For additional information please contact:
ACSIS@davidson-tech.com

Collaboration to Develop IP/Discriminator

Small Business Partnerships

Program Development Support

Architecture and System Development

Comprehensive Regulation Knowledge

Life-Cycle Value Added

Opportunity Shaping

Customer Relationships

Vendor Relationships

IAMD/BMDS Domain Knowledge

Davidson Technologies
Missiles • Aerospace • Cyber • Intelligence