



Summary of: Assessments & Evaluation, Experiments & Pilots, and Transition to Practice

CSD PI Meeting, October 2012

**Scott Tousley, Greg Wigton,
Mike Pozmantier**

Cyber Security Division

**Homeland Security Advanced
Research Project Agency**

Scott.Tousley@hq.dhs.gov,

Gregory.Wigton@hq.dhs.gov,

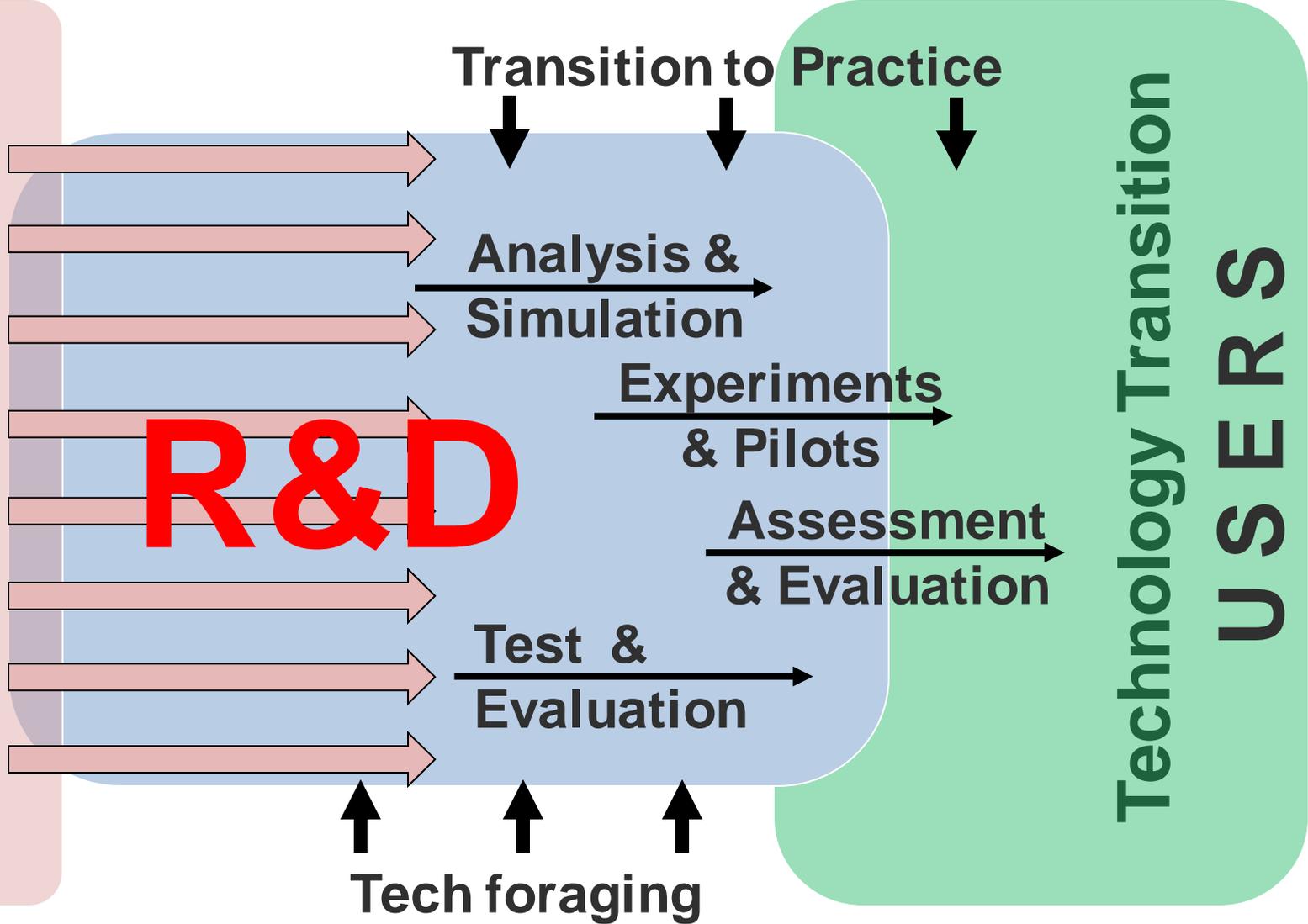
Mike.Pozmantier@hq.dhs.gov

CSD R&D structure concept

6.2 ← CSD Work Areas → 6.7

R&D Strategy

CSD Programs & Projects





Assessment & Evaluation



- Description
 - Conduct red team evaluations, systems assessment, and risk analysis, supporting development & implementation of cyber security technologies
 - Promote public/private partnerships to facilitate transitioning of technologies through engagement with the private sector through Infosec Technology Transition Council (ITTC) and Security Innovation Network's (SINET) conferences and workshops
- Technical Assessment
 - Use two different red team organizations (Sandia, Exelis)
 - Technology and A&E PM's collaborate on the testing specifics
- Business Assessment
 - Establish multiple opportunities for business/technical consideration across the cyber investment community
 - DOD/DHS SBIR Conf., SINET, ITTC, Value creation workshops



Assessments summary



Technology	Type	Sponsor	Deployment	Tested
MOZART	Website Analysis	Air Force IOB	Federal Law Enforcement Agency, Miami, FL	Spring 2007
IronKey	Secure Storage	DHS S&T	Local Police Depart., Utica, NY	Spring 2008
Zippy Report Tool	Cell Phone Forensics	COTS	Local Police Dept., Utica, NY	Spring 2008
CAULDRON	Vulnerability Assessment	DHS S&T	Small College, Utica, NY	Fall 2008
kHIVE	Rootkit Detection	DHS S&T	U.S. Secret Service: Miami, FL and Washington, DC, & Syracuse NY	Fall 2008, Fall 2009
FATMAN	Malware Analysis	AFRL	Local Police Dept., Utica, NY; U.S. Secret Service, Washington, DC	Summer, Fall 2009
CAULDRON	Vulnerability Assessment	DHS S&T	U.S. Secret Service, Washington, DC	Winter 2010, Winter 2011
Responder Pro	Malware Analysis	DHS S&T	ITT IS, IT Security Operations Center	Spring 2010
OneWireless	SCADA Mesh Network	DHS S&T/Critical Infrastructure	Pre-deployment	Spring 2010



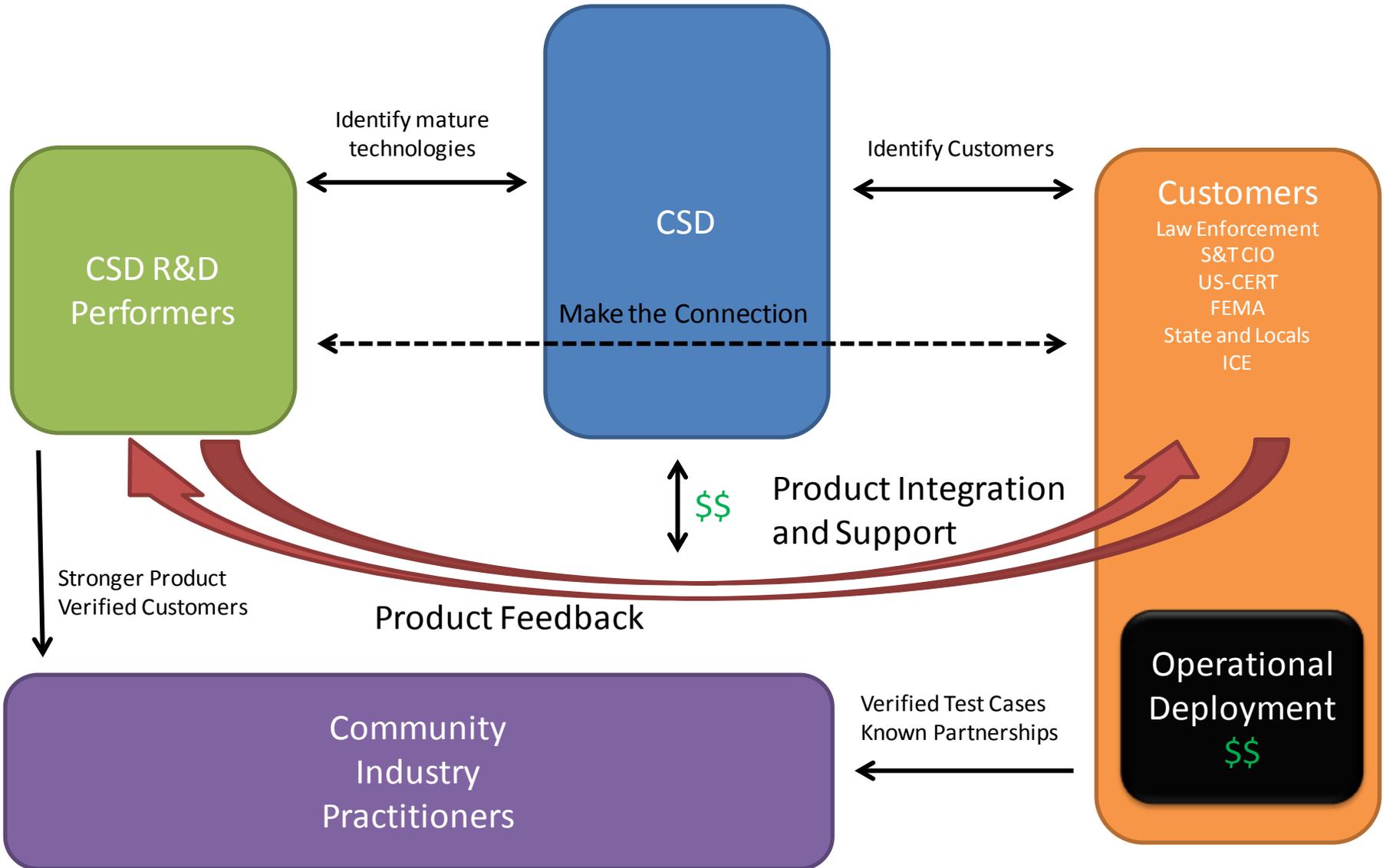
Assessments summary (2)



Technology	Type	Sponsor	Deployment	Tested
Damballa FailSafe	Botnet Detection and Mitigation	DHS S&T	Deployment Site Omitted For Security Purposes	Fall 2010
DECIDE	Simulation, training & exercise code	DHS S&T	TBD	Spring 2011
VIAssist	Advanced Visualization	DHS S&T	Deployment Site Omitted For Security Purposes	Winter 2011
DETER Federation	Infrastructure/Test bed	DHS S&T	Multiple DETER node locations	Spring 2012
ADF Responder	Live Forensic Acquisition	DHS S&T	Local Police Dept., Utica, NY	Spring 2012
CFTT Validation Test Plans	Computer Forensic Tool Validation	NIST	CyberFETCH Web Environment	Ongoing
Forensic Triage Standard	Capabilities standard/matrix	NIST	CyberFETCH Web Environment	Ongoing
SingleKey	Application Layer Firewall	Bayshore	Exelis IT-SOC and US Coast Guard	Planning



Experiments and Pilots Operational Context





Customers



- Past Customers
 - Federal Law Enforcement Training Center (FLETC)
 - Law Enforcement Agencies
 - DHS S&T CIO
 - State and Locals
 - US Computer Emergency Readiness Team (US-CERT)
- Planned Future Customers
 - United States Secret Service (USSS)
 - Library of Congress CISO
 - DHS CISO Council
 - Federal Emergency Management Agency (FEMA)
 - Immigration and Customs Enforcement (ICE)
 - Nuclear Regulatory Commission (NRC)



Successful Experiments and Pilots

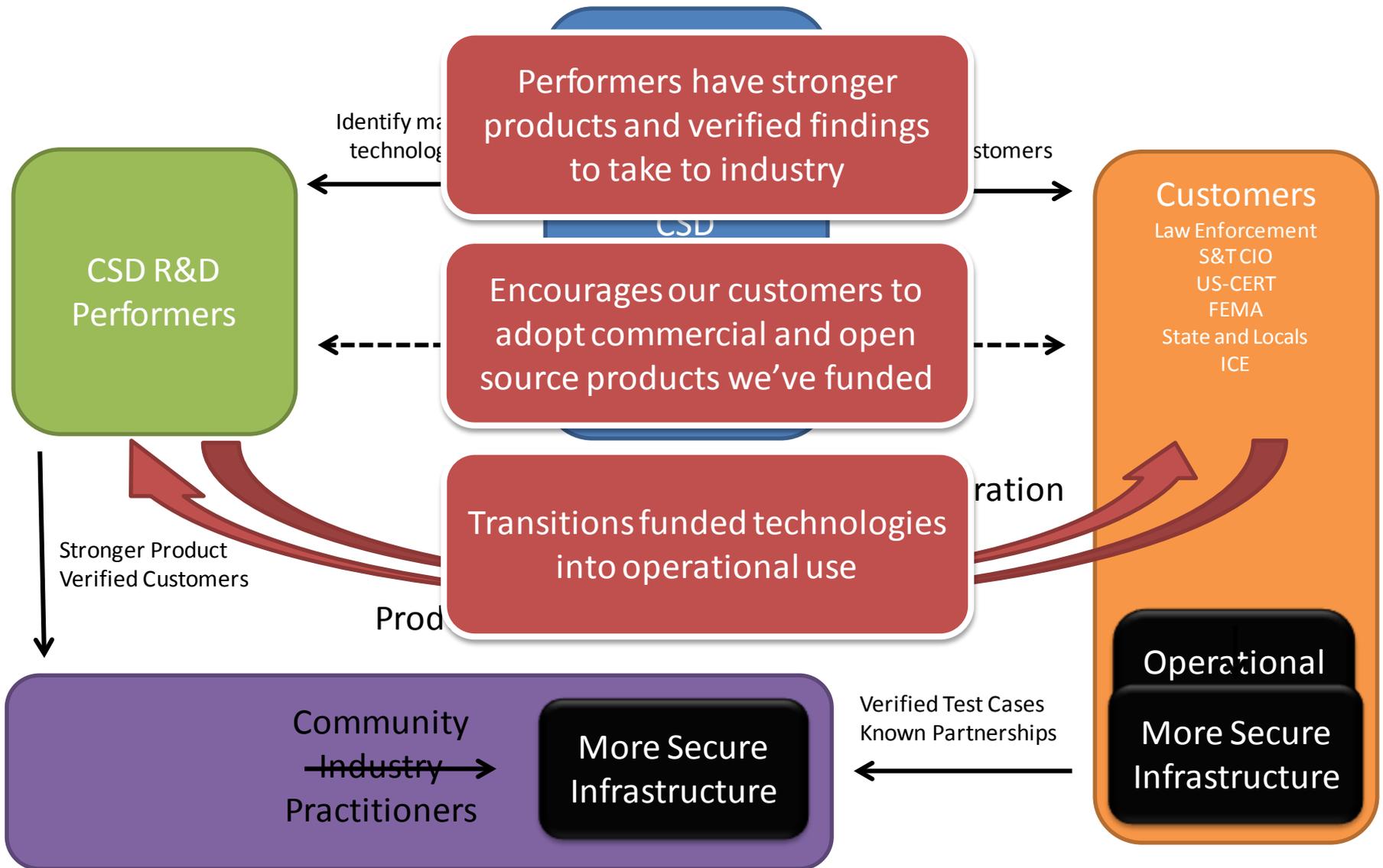


- Cyber Scenario Modeling And Reporting Tool (CyberSMART)
 - Initial version used in two state exercises
 - MassAttack (MA)
 - Emerald Down (WA)
- Botnet Detection and Mitigation Tool
 - Deployed by the State of Washington in their PRISEM IT Infrastructure
- Ironkey Secure USB
 - Transitioned into a commercial product and is used by Government agencies and Industry
- HBGary Forensics Tool
 - Used by Law Enforcement agencies





Experiments and Pilots – Value





TTP Program Focus Areas



Identify

- Identify federally funded cyber security research that is at Technical Readiness Level (TRL) 5 or higher that can be projected into the Homeland Security Enterprise and beyond

Implement

- Partner with the IT operations groups within the Homeland Security Enterprise to pilot the cybersecurity technologies that are identified

Introduce

- Partner with the private sector to commercialize technology to bring the innovation to a broader audience



TTP Focus Areas Defined



R&D Sources

- DOE National Labs
- FFRDC's (Federally Funded R&D Centers)
- Academia

Transition processes

- Testing & evaluation
- Red Teaming
- Pilot deployments

Utilization

- Open Sourcing
- Licensing
- New Companies
- Adoption by cyber operations analysts
- Direct private-sector adoption
- Government use



TTP Activities



- Tech Foraging
 - Travel to National Labs to meet researchers and view demonstrations of mature cybersecurity research
- Networking
 - Attend conferences and workshops
 - Brief industry organizations such as CTIA – The Wireless Association and Bay Area Council on Transition to Practice
- Demonstrate Technology
 - Hold Demonstration Days for critical infrastructure sectors:
 - Federal Government
 - Financial Industry
 - Others



TTP Activities (cont.)



- Test and Evaluation and Red Teaming
 - TTP will fund the Test and Evaluation and Red Teaming of all technologies it works with, to confirm and improve
- Piloting
 - Work with the public and private sector to pilot technology in production environments
- Funding
 - Fund improvements to promising technologies
 - Assist in funding pilots, and transition to market
- Catalogs
 - Work w/research partners to produce Cyber Research Catalog
 - Work w/operational partners to produce listing of Cyber Gaps