Homeland Security
Science and Technology

Transition to Practice Overview FY13 PI Meeting

Michael Pozmantier
Program Manager – Transition to Practice
Cyber Security Division
DHS Science and Technology
michael.pozmantier@hq.dhs.gov

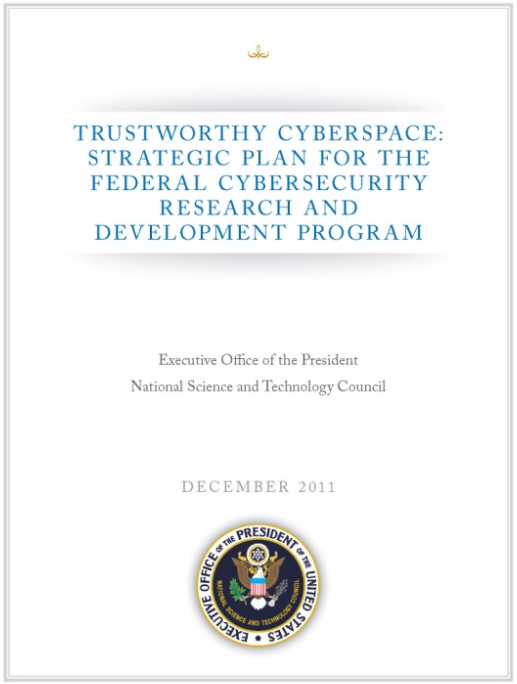
September 16, 2013

$1,000,000,000

Source – NITRD Supplement to the President's FY13 and FY14 Budget; specifically covering Program Component Areas (PCAs): Cybersecurity and Information Assurance (CSIA), High-Confidence Software and Systems (HCSS) Large-Scale Networking (LSN), Software Design and Productivity (SDP)

Homeland Security
Science and Technology

Transition to Practice


TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

Executive Office of the President
National Science and Technology Council

DECEMBER 2011


the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATI

Home ▪ Briefing Room ▪ Presidential Actions ▪ Presidential Memoranda

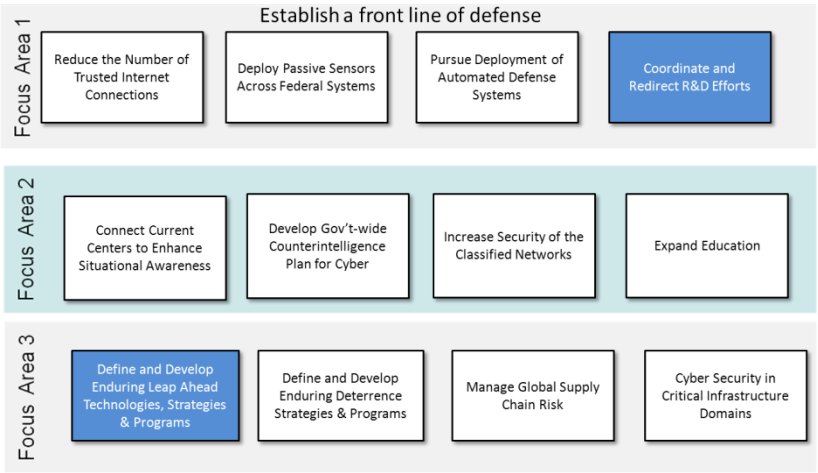
The White House
Office of the Press Secretary

E-Mail | Tweet | Share

For Immediate Release — October 28, 2011

Presidential Memorandum -- Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES




the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATI

Home ▪ Briefing Room ▪ Presidential Actions ▪ Executive Orders

The White House
Office of the Press Secretary

E-Mail | Tweet | Share

For Immediate Release — February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Homeland Security
Science and Technology

Overarching Goals of TTP

1. Promote the CSD methodology so that Technology Transition becomes an early and continuing focus, thus shortening the time it takes to go from the lab to the marketplace

2. TTP will become a connection point for the research community, cybersecurity professionals and private sector:
   - Researchers can use TTP to find operational partners for input and pilots
   - Cyber professionals can find emerging technologies to meet their operational needs more easily
   - Private sector can more easily find innovation to license and invest in

Homeland Security
Science and Technology

TTP Program Focus Areas

Identify

- Identify federally funded cyber security research that is pilot-ready and can be projected into the Homeland Security Enterprise

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

Homeland Security
Science and Technology

TTP Focus Areas Defined

R&D Sources

- DOE National Labs
- DOD FFRDC's
- Academia

Transition processes

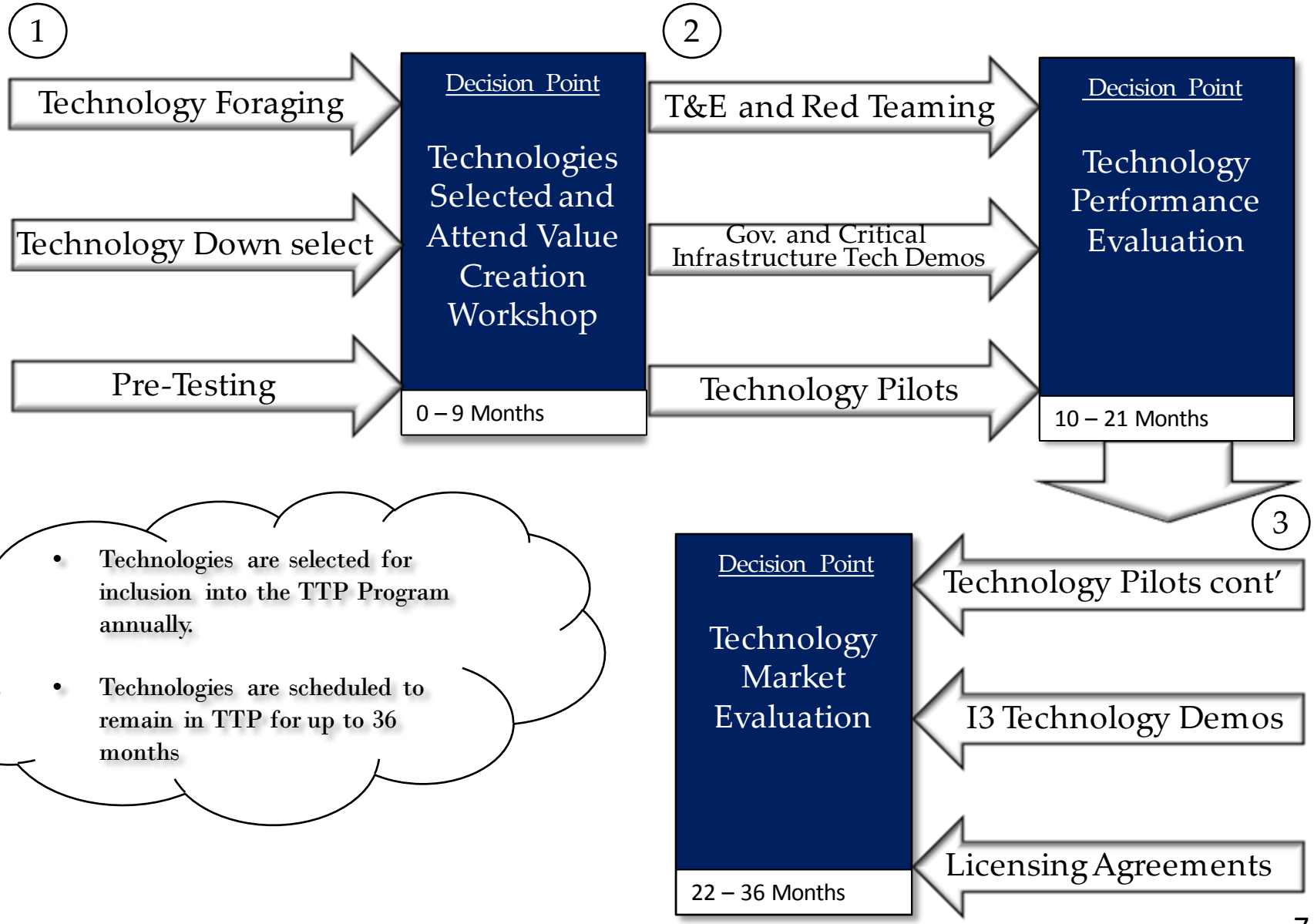
- Testing & evaluation
- Red Teaming
- Pilot deployments

Utilization

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

Homeland Security
Science and Technology

TTP Program Cycle



Homeland Security
Science and Technology

TTP World Tour FY12

Pacific Northwest National Lab (PNNL)	April 17
Lawrence Livermore National Lab (LLNL)	April 18
Sandia National Lab – Livermore (SNL)	April 19
Lawrence Berkeley National Lab (LBL)	April 20
Oak Ridge National Lab (ORNL)	May 14
Los Alamos National Lab (LANL)	May 16
Sandia National Lab – Albuquerque (SNL)	May 17
Argonne National Lab (ANL)	June 12

Los Alamos NATIONAL LABORATORY

Sandia National Laboratories

Lawrence Livermore National Laboratory

Argonne NATIONAL LABORATORY

Pacific Northwest NATIONAL LABORATORY

OAK RIDGE National Laboratory

BERKELEY LAB Lawrence Berkeley National Laboratory

Homeland Security
Science and Technology

Summary of Identified Technologies FY12

Technology	Lab	Description
Path Scan	LANL	Intrusion Detection. Detects anomalous multi-hops to find attacks. Based on general hacker behavior of traversing networks once they gain a foot hold.
Code Seal	SNL	Trust anchors. Distributed, encrypted processing that obfuscates functions in untrusted environments.
Net_Mapper / Everest	LLNL	Network mapping and visualization tool. Active and Passive mapping, light weight.
MLSTONES	PNNL	Biology based malware and event analysis. Utilizes user defined buckets, like amino acids, that tag events and sequence them. Algorithm looks for similarities that it will match to find the same or similar strings of events.
Hone	PNNL	Network traffic analysis. Inspects the network and transport layers of packets to map process with port and IP.
Hyperion/FX	ORNL	Malware detection, software assurance. Use binary to calculate software behavior with mathematical certainty.
Choreographer	ORNL	Moving target defense. Uses NAT to shift server IP's replacing them with honey pots. Able to detect when a connection has bypassed DNS to shift it seamlessly to a honeypot.
USB ARM	ORNL	Removable media policy enforcement. Prevents removable media (USB, DVD, etc.) from mounting into file system so device can be scanned or analyzed. Detects Windows executables allowing for white or black listing.

Homeland Security
Science and Technology

TTP World Tour FY13

Pacific Northwest National Lab (PNNL)	April 15
Lawrence Berkeley National Lab (LBL)	April 16
Lawrence Livermore National Lab (LLNL)	April 16
Sandia National Lab – Livermore (SNL)	April 17
Johns Hopkins Applied Physics Lab (JHU-APL)	May 16
Oak Ridge National Lab (ORNL)	May 20
SPAWAR Systems Center – Pacific (SSC-P)	June 3
Los Alamos National Lab (LANL)	June 5
Sandia National Lab – Albuquerque (SNL)	June 6
MIT-Lincoln Labs (MIT-LL)	June 27

Homeland Security
Science and Technology

Summary of Identified Technologies FY13

Technology	Lab	Description
CodeDNA	JHU-APL	Malware Detection; Provides a reliable, fully automated, fast means for identifying related malware binaries and linking variants
Quantum Security	LANL	Security Based on the Laws of Physics; Two tools: Quantum Secure Communications replaces PKI and a quantum random number generator (Velocirandor) provides true random bits at high rates
CryptAC	MIT-LL	Cloud Data Security; provides cryptographic access control, enabling secure storage of data in public clouds
LOCKMA	MIT-LL	Key Management Architecture; software component designed to significantly simplify the task of adding cryptographic protections and underlying key management to software, among other use cases
Digital Ants	PNNL	Bio-inspired Cybersecurity; Uses dynamic, decentralized ant-like sensor programs to provide mobile, resilient cyber security by detecting anomalies
PACRAT	PNNL	Physical And Cyber Risk Analysis Tool; Provides a comprehensive modeling and simulation capability that can evaluate every avenue of approach - using both electronic and physical pathways
Serial Tap	PNNL	Control System Security; Passive in-line device that collects serial communication and transits it as a secure UDP packet
SecuritySeal	SNL	Supply Chain Security; Leverages Physical Unclonable Functions (PUFs) to create physical seals that can be used to verify that a system is authentic
Weasel Board	SNL	Programmable Logic Controller Security; provides zero-day exploit protection for PLCs by capturing and analyzing backplane traffic

Homeland Security
Science and Technology

TTP Upcoming Events

- Tech Demo Day for Integrator, Investor and IT Companies –East
  - Washington, DC – October 9, 2013
- 2nd Annual Federal Government Tech Demo Day
  - Washington, DC - November 8, 2013
- Tech Demo Day for the Energy Sector
  - Houston, TX – February/March 2014
- Tech Demo Day for the Finance Sector
  - New York, NY – May/June 2014

Thank you!

Successful Technology Transition
Salon A/B
4:35pm-5:35pm