CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS' MEETING

Crystal Gateway Marriott | Arlington VA

September 16 – 18, 2013

Homeland Security

Science and Technology

Meeting Logistics

- **Registration:** Check-in will begin at 7:30 a.m. daily. Please sign-in each day.
- **General Session:** Begins daily at 8:30 a.m.
- **Restrooms:** Located across from Salon A.
- **Wi-Fi Access:** Please limit access to one personal device
  Network: ibahn_conference
  Password: 09959d
- **Beverage Service:** Water stations will be in the Grand Ballroom Foyer. Coffee and other beverages are available at Einstein Bagels, located on the *Lobby Level.*
- **Lunch:** is on your own. Listing of nearby eateries (page 2) of the attendee packet

Meeting Logistics

- **Presentation Slides**: Available at the PI meetings website http://events.SignUp4.com/2013CyberPIMeeting
- **Q&A:** Questions must be spoken into the microphones. This will allow webcast attendees to hear the questions.
- **End of The Day Wrap-Up:** Please return your badge to the registration desk
- **Survey:** Please complete the electronic survey rating your experience at the CSD 2013 PI Meeting. https://www.surveymonkey.com/s/CSD_2013_PI_Meeting_Survey
- **Questions?:** Please see the registration desk.

Live Webcast

- **Webcast Link:**
  http://dhs.bizvision.com/2013CyberPIwebcast-registration

  If you've already registered:
  http://dhs.bizvision.com/2013CyberPIwebcast

- General Session and Technical Tracks will be webcast

- The webcasted videos will also be available for viewing through the above link after the PI meeting.

- If you require any technical support, please contact the BizVision Helpdesk at 1-800-747-1719 or support@bizvision.com

Homeland Security Advanced Research Projects Agency

S&T's Role in Cyber Security and the Way Forward

September 16, 2013

DHS S&T Principal Investigator Meeting

Douglas Maughan
Division Director

http://www.cyber.st.dhs.gov

Homeland Security
Science and Technology

Homeland Security
Science and Technology

Presentation Outline

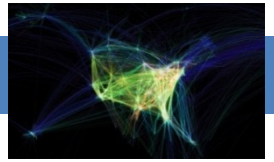
- Why We Are Here
- International Involvement
- National / Federal Activities
- DHS Activities
- Cyber Security Division (CSD) Overview
- What’s Ahead
- Summary
- Administrative Items
- Q&A

Environment: Greater Use of Technology, More Threats, Less Resources

Homeland Security
Science and Technology

Globalization & Transportation


Anywhere in the world in 24 hours

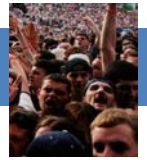


Border Security & Immigration

Tenuous balance


Violent Extremism





Insider Threat

Cyber Domain

Low cost of entry

Strategic potential

Nature of Innovation

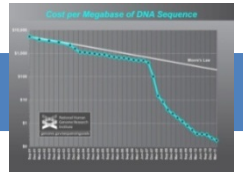
Both sides get to innovate

Predictive & Reactive

Aviation as an example …

Misuse of Technology

Historical Perspective

Natural Disasters & Pushing Beyond Design Limits




LESS RESOURCES

MORE THREATS

Homeland Security
Science and Technology

Cyberspace Definitions

"Cyberspace is [our nation's critical infrastructures'] nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work." ***National Strategy to Secure Cyberspace, 2003***

"Cyberspace means the interdependent network of IT infrastructures, and includes the internet, telecomms networks, computer systems, and embedded processors and controllers in critical industries" ***NSPD 54, 8 Jan 2008***

"A cyber environment includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks. ***International Telecommunications Union X.1205, Overview of Cybersecurity, Oct 2008***

"The terms cyber security and information assurance refer to measures for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification, or destruction." ***Federal Plan for Cyber Security and Information Assurance Research and Development, Apr 2006***

Homeland Security
Science and Technology

Cyberspace Definitions

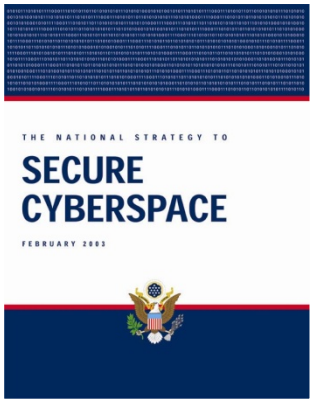
"The interdependent network of information and communications technology infrastructures, including the Internet, telecommunications networks, computer systems and networks, and embedded processors and controllers in facilities and industries." **White House Cyberspace Policy Review, May 2009**

AND PEOPLE!!!

Homeland Security
Science and Technology

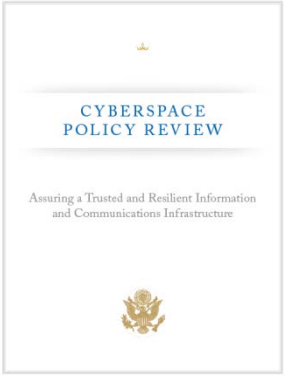
Cybersecurity Requirements Historical Timeline

2003



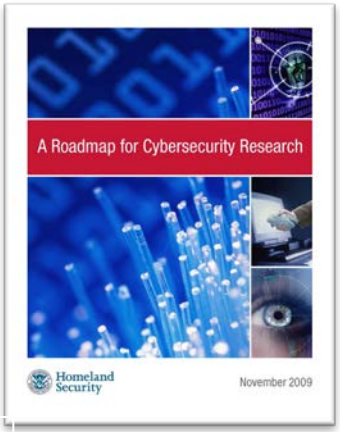
Call for Action
-Secure Protocols
DNSSEC
Secure Routing
-DETER security testbed
- PREDICT data repository

2008



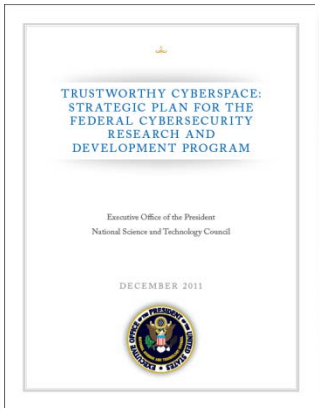
Beginnings of CNCI
- Call for NICE (Education)
- Call for NSTIC (Trusted Identities)
- Reinforced need for PREDICT data repository

2009



S&T Produced National R&D community input
Source for DHS S&T BAA, SBIR, and other solicitations

2011



CNCI Tasks 4&9
S&T led via co-chair of CSIA IWG
Significant inter-agency activities (More later)

2012

Implementation plan to accomplish goals of DHS QHSR
24 high priority capabilities needed
NPPD-led, S&T involved
RFI intended to guide S&T's future investments

Ongoing

EO – 13636

PPD - 21

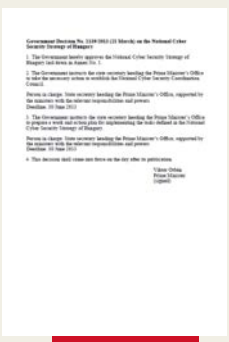
CNCI Way Forward

Cybersecurity Strategies – International (1 of 2)

Slovakia

Switzerland

United Kingdom



Hungary

Japan

USA

Luxembourg

India

Uganda

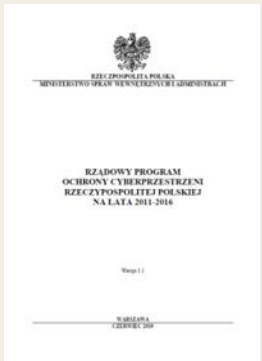
South Africa

European Union

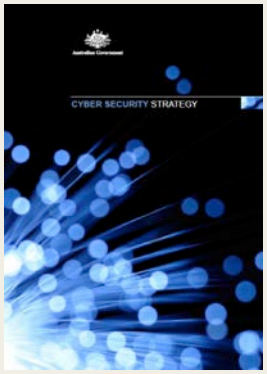
Poland

Romania

Russia



Cybersecurity Strategies – International (2 of 2)

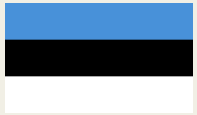


Austria

Australia

Canada

Czech Republic



Estonia

New Zealand

Finland

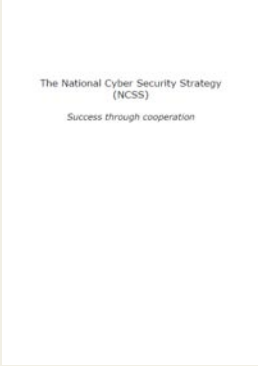
France

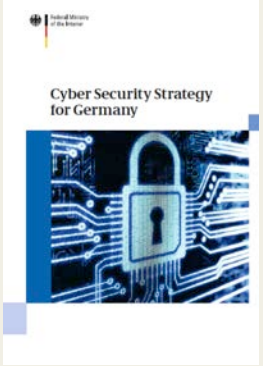
Netherlands

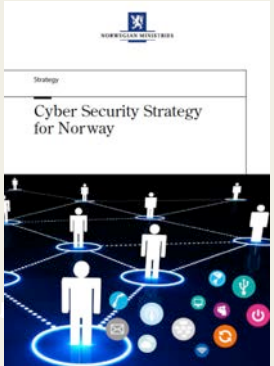
Germany

Lithunia

Norway







Comprehensive National Cybersecurity Initiative (CNCI)

Focus Area 1

Establish a front line of defense

- Reduce the Number of Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Automated Defense Systems
- Coordinate and Redirect R&D Efforts

Focus Area 2

Resolve to secure cyberspace / set conditions for long-term success

- Connect Current Centers to Enhance Situational Awareness
- Develop Gov't-wide Counterintelligence Plan for Cyber
- Increase Security of the Classified Networks
- Expand Education

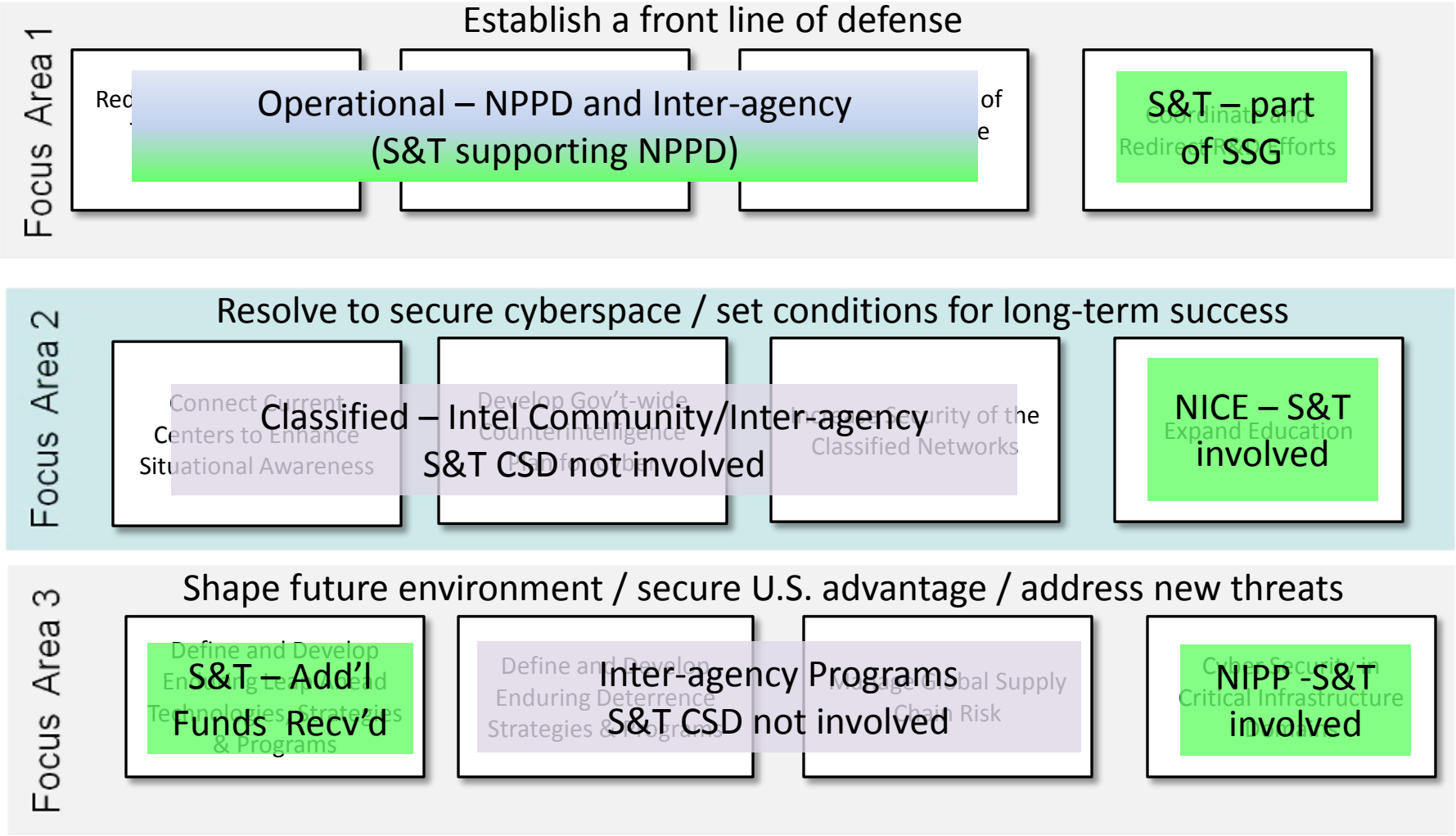
Focus Area 3

Shape future environment / secure U.S. advantage / address new threats

- Define and Develop Enduring Leap Ahead Technologies, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Manage Global Supply Chain Risk
- Cyber Security in Critical Infrastructure Domains

http://cybersecurity.whitehouse.gov

Comprehensive National Cybersecurity Initiative (CNCI)



http://cybersecurity.whitehouse.gov

U.S. Federal Cybersecurity Operations Team

National Roles and Responsibilities

US Government Departments and Agencies

DOJ/FBI

- Investigate, attribute, disrupt and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

DHS

- Coordinate the national protection, prevention, mitigation of, and recovery from cyber incidents
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigate cyber crimes under DHS's jurisdiction

DoD

- Defend the nation from attack
- Gather foreign cyber threat intelligence and determine attribution
- Secure national security and military systems
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Investigate cyber crimes under military jurisdiction

Global Cyberspace

Coordinate with Public, Private, and International Partners

** Note: Nothing in this chart alters existing DOJ, DHS, and DoD roles, responsibilities, or authorities*

UNCLASSIFIED

Homeland Security
Science and Technology

NITRD Participating Agencies

NNSA National Nuclear Security Administration

U.S. Department of Homeland Security

National Science Foundation

National Institutes of Health

NIST National Institute of Standards and Technology

DARPA

NITRD

NOAA National Oceanic and Atmospheric Administration, U.S. Department of Commerce

United States Environmental Protection Agency

Networking Information Technology R&D

Department of Defense, United States of America

National Security Agency, United States of America

NASA

Office of Science, U.S. Department of Energy

AHRQ

The National Archives, Archives.gov, Democracy Starts Here.

Federal Cybersecurity R&D Strategic Plan

- Science of Cyber Security
- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target Defense
  - Cyber Economics and Incentives
  - Designed-In Security (New for FY13)
- Transition to Practice
  - Technology Discovery
  - Test & Evaluation / Experimental Deployment
  - Transition / Adoption / Commercialization
- Support for National Priorities
  - Health IT, Smart Grid, NSTIC (Trusted Identity), NICE (Education), Financial Services


the WHITE HOUSE PRESIDENT BARACK OBAMA

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

Home • The Administration • Office of Science and Technology Policy

Office of Science and Technology Policy

About OSTP | OSTP Blog | Pressroom | Divisions | R&D Budgets | Resource Library | NSTC

Federal Cybersecurity R&D Strategic Plan Released

Subscribe

Posted by Aneesh Chopra and Howard Schmidt on December 06, 2011 at 12:38 PM EST

E-Mail | Tweet | Share

Today, OSTP is releasing *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*—a road map to ensuring long-term reliability and trustworthiness of the digital communications network that is increasingly at the heart of American economic growth and global competitiveness.

Early in his Administration, the President ordered a top-to-bottom review of the Government's cyberspace policy. The resulting *Cyberspace Policy Review* challenged Federal agencies to develop a targeted set of cybersecurity research priorities to "change the game" so that cyberspace can become safer and more trustworthy—key to facilitating continued growth of the Nation's digital infrastructure. The cybersecurity R&D strategic plan being released today is in direct response to the near-term action plan of the *Cyberspace Policy Review* and seeks to enhance and focus our cybersecurity research and development efforts by setting forth coordinated Federal

Released Dec 6, 2011

http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released

Homeland Security
Science and Technology

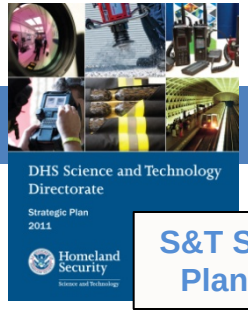
DHS S&T Mission Guidance

Strategic Guidance

Homeland Security Act 2002

QHSR (Feb 2010)

BUR (July 2010)



S&T Strategic Plan (2011)

QHSR

Threats

- Smaller Scale Terrorism
- Trafficking, Crime
- Pandemics, Accidents, Natural Hazards
- Violent Extremism
- High Consequence WMD

Core Missions

1. Preventing terrorism & enhancing security
2. Securing and managing our borders
3. Enforcing & administering immigration laws
4. Safeguarding and securing cyberspace
5. Ensuring resilience to disasters

Operational Directives

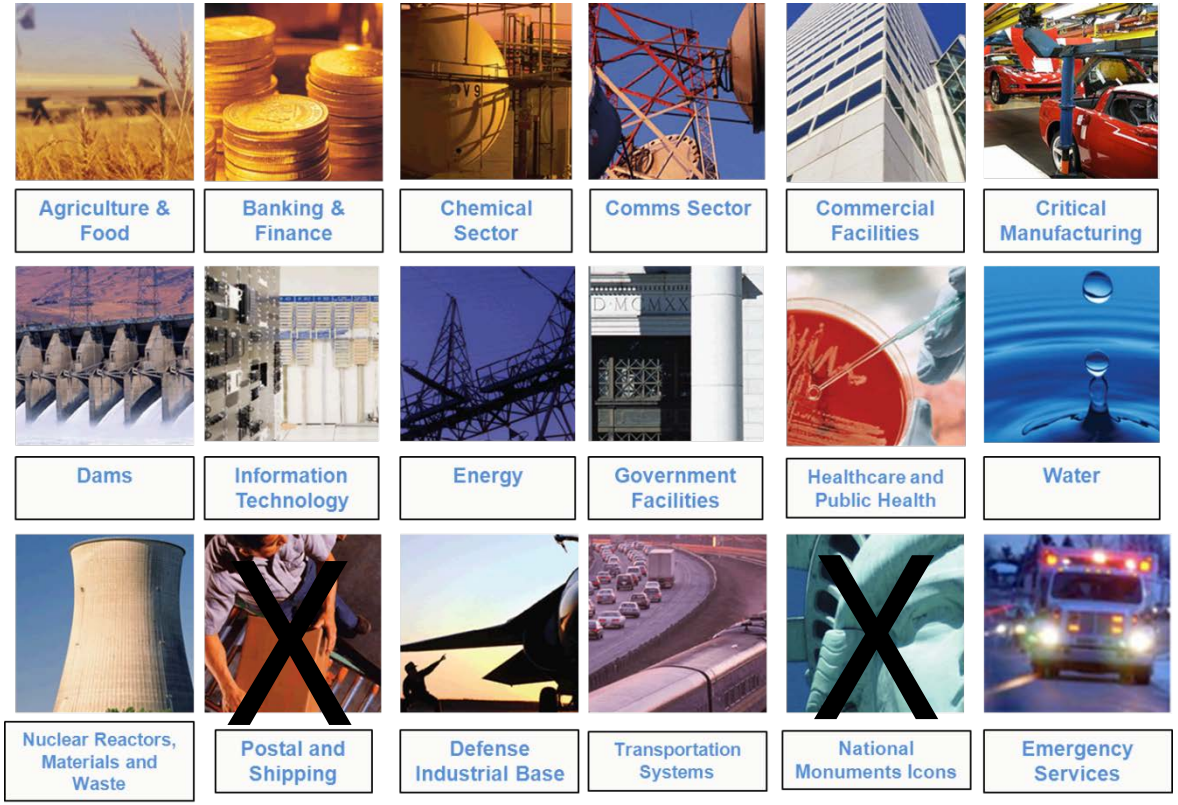
- HSPD-5 National Incident Management System (2003)
- HSPD-9 Defense of U.S. Agriculture & Food (2004)
- HSPD-10 Biodefense for the 21st Century (2004)
- HSPD-22 Domestic Chemical Defense (2007)
- PPD-8 National Preparedness (2011)

Prevention, Protection, Mitigation, Response, Recovery

Cybersecurity for the 16 Critical Infrastructure Sectors

Homeland Security
Science and Technology

DHS provides advice and alerts to the 16 critical infrastructure areas …



… DHS collaborates with sectors through Sector Coordinating Councils (SCC)

<u>In the future, DHS will provide cybersecurity for …</u>

- ❑ **The .gov and critical .com domains with a mix of:**
  - ➢ **Managed security services**
  - ➢ **Developmental activities**
  - ➢ **Information sharing**
- ❑ **Linkages to our U.S. – CERT (Computer Emergency Readiness Team)**

National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center for production of a common operating picture …

Homeland Security
Science and Technology

EO-13636 and PPD-21

- In February 2013, the President issued two new policies:
  1) Executive Order 13636: Improving Critical Infrastructure Cybersecurity
  2) Presidential Policy Directive – 21: Critical Infrastructure Security and Resilience
- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems

Homeland Security
Science and Technology

Integrating Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security

- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - **Develop comprehensive research and development plan (CSD / RSD)**

DHS S&T Mission

Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise

1) Create new technological capabilities and knowledge products
2) Provide Acquisition Support and Operational Analysis
3) Provide process enhancements and gain efficiencies
4) Evolve US understanding of current and future homeland security risks and opportunities

FOCUS AREAS

- Bio
- Explosives
- Cybersecurity
- First Responders
- Resilient Systems
- Borders / Maritime

Homeland Security
Science and Technology

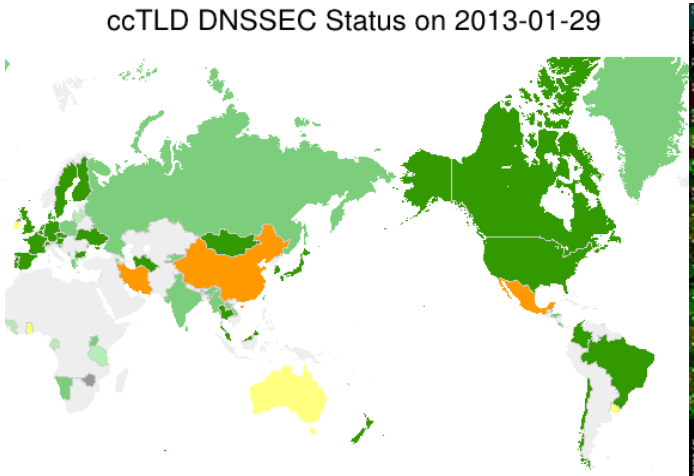
Homeland Security
Science and Technology

Cyber Security Focus Areas

- Trustworthy Cyber Infrastructure
  - Working with the global Internet community to secure cyberspace
- Research Infrastructure to Support Cybersecurity
  - Developing necessary research infrastructure to support R&D community
- R&D Partnerships
  - Establishing R&D partnerships with private sector, academia, and international partners
- Innovation and Transition
  - Ensuring R&D results become real solutions
- Cybersecurity Education
  - Leading National and DHS cybersecurity education initiatives

Trustworthy Cyber Infrastructure

- Secure Protocols
  - DNSSEC – Domain Name System Security
    - Govt and private sector worked together to make this happen
    - Started in 2004; now 111 top level (gTLD) and country code (ccTLD) domains adopted globally including the Root
  - SPRI – Secure Protocols for Routing Infrastructure
- Internet Measurement and Attack Modeling
  - Geographic mapping of Internet resources
  - Logically and/or physically connected maps of Internet resources
  - Monitoring and archiving of BGP route information
  - Co-funding with Australia



http://www.isi.edu/ant/address/browse/

Research Infrastructure (RISC)

- Experimental Research Testbed (DETER)
  - Researcher and vendor-neutral experimental infrastructure
    - Used by over 200 organizations from more than 20 states and 17 countries
    - Used by over 40 classes, from 30 institutions involving 2,000+ students
  - http://www.deter-project.org
- Research Data Repository (PREDICT)
  - Repository of network data for use by the U.S.- based cyber security research community
    - More than 200 users (academia, industry, gov't); Over 600TB of network data; Tools are used by major service providers and many companies
    - Phase 2: New datasets, ICTR Ethics, International (CA, AUS, JP, EU)
  - https://www.predict.org
- Software Assurance Market Place (SWAMP)
  - A software assurance testing and evaluation facility and the associated research infrastructure services

Homeland Security
Science and Technology

R&D Partnerships

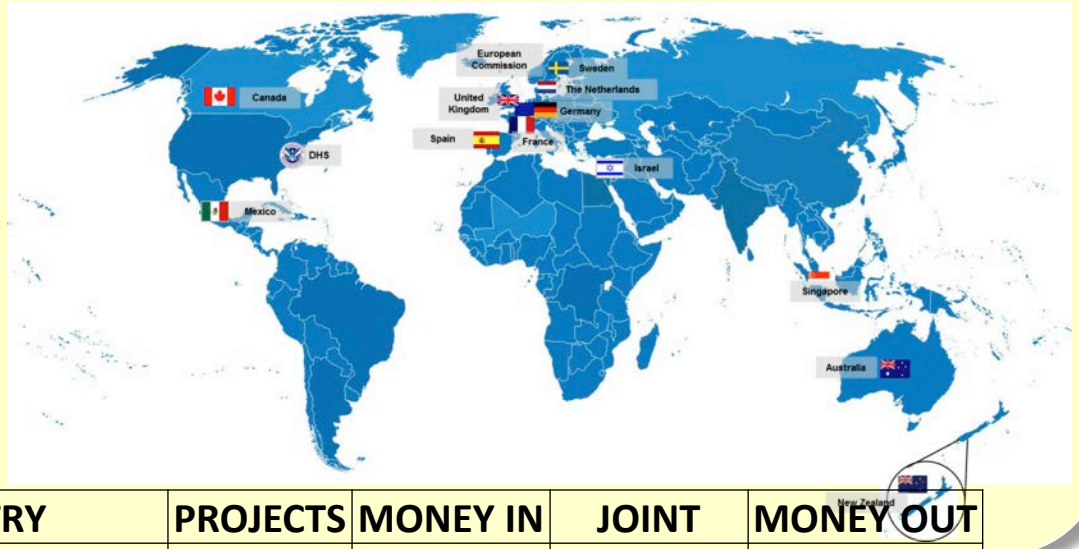
- Oil and Gas Sector
  - LOGIIC – Linking Oil & Gas Industry to Improve Cybersecurity
- Electric Power Sector
  - TCIPG – Trustworthy Computing Infrastructure for the Power Grid
- Banking and Finance Sector
  - FI-VICS – Financial Institutions – Verification of Identity Credential Service
  - DECIDE – Distributed Environment for Critical Incident Decision-making Exercises (recent Quantum Dawn II exercise)
- State and Local
  - PRISEM - Public Regional Information Security Event Management
  - PIV-I/FRAC TTWG – State and Local and Private Sector First Responder Authentication Credentials and Technology Transition
- Law Enforcement
  - SWGDE – Special Working Group on Digital Evidence (FBI lead)
  - CFWG – Cyber Forensics Working Group (CBP, ICE, USSS, FBI, S/L)

S&T International Engagements

❑ International Bilateral Agreements

➢ **Government-to-government cooperative activities for 13 bilateral Agreements**

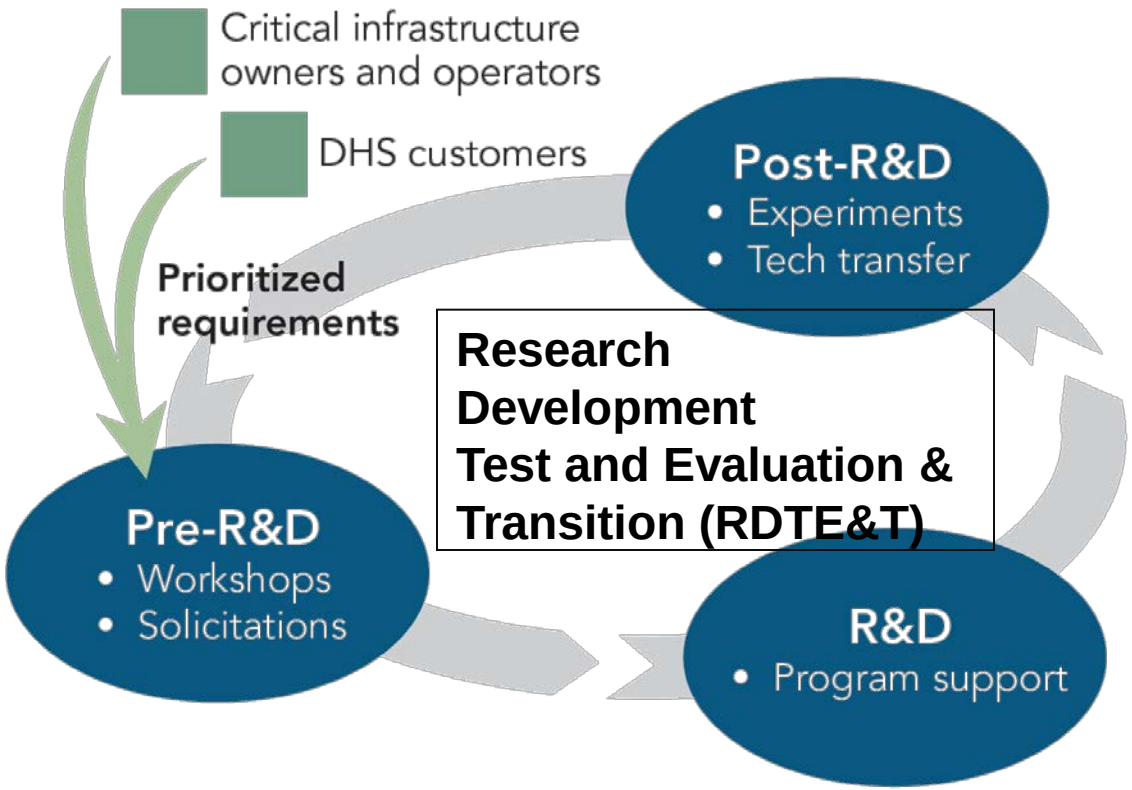
- **Canada (2004)**
- **Australia (2004)**
- **United Kingdom (2005)**
- **Singapore (2007)**
- **Sweden (2007)**
- **Mexico (2008)**
- **Israel (2008)**
- **France (2008)**
- **Germany (2009)**
- **New Zealand (2010)**
- **European Commission (2010)**
- **Spain (2011)**
- **Netherlands (2013)**



Over $6M of International co-funding

COUNTRY	PROJECTS	MONEY IN	JOINT	MONEY OUT
Australia	3	$300K	$400K	
Canada	11	$1.8M		
Germany	1		$300K	
Israel	2		$100K	
Netherlands	7	$450K	$1.2M	$150K
Sweden	4	$650K		
United Kingdom	3	$1.2M	$400K	
European Union	1			
Japan	1			

CSD R&D Execution Model



Example: DARPA has provided $9M to CSD for development and transition of Military Networking Protocol (MNP) technology and has started discussions for testing and evaluation of Automated Malware Analysis technology

Successes

- Ironkey – Secure USB
  - Standard Issue to S&T employees from S&T CIO
  - Acquired by Imation
- Komoku – Rootkit Detection Technology
  - Acquired by Microsoft
- HBGary – Memory and Malware Analysis
  - Over 100 pilot deployments as part of Cyber Forensics
- Endeavor Systems – Malware Analysis tools
  - Acquired by McAfee
- Stanford – Anti-Phishing Technologies
  - Open source; most browsers have included Stanford R&D
- Secure Decisions – Data Visualization
  - Pilot with DHS/NCSD/US-CERT; Acquisition

Cyber Security R&D Broad Agency Announcement (BAA)

- Delivers both near-term and medium-term solutions
  - To **develop new and enhanced technologies** for the detection of, prevention of, and response to cyber attacks on the nation's critical information infrastructure, based on customer requirements
  - To perform research and development (R&D) aimed at **improving the security of existing deployed technologies** and to ensure the security of new emerging cybersecurity systems;
  - To **facilitate the transfer of these technologies** into operational environments.

- Proposals Received According to 3 Levels of Technology Maturity

Type I (New Technologies)
- ✓ Applied Research Phase
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ $3M & 36 mos.

Type II (Prototype Technologies)
- ✓ More Mature Prototypes
- ✓ Development Phase
- ✓ Demo in Op Environ.
- ✓ Funding ≤ $2M & 24 mos.

Type III (Mature Technologies)
- ✓ Mature Technology
- ✓ Demo Only in Op Environ.
- ✓ Funding ≤ $750K & 12 mos.

Note: Technology Demonstrations = Test, Evaluation, and Pilot deployment in DHS "customer" environments

Homeland Security
Science and Technology

Homeland Security
Science and Technology

Transition To Practice (TTP) Program

R&D Sources

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

Transition processes

- **Testing & evaluation**
- **Red Teaming**
- **Pilot deployments**

Utilization

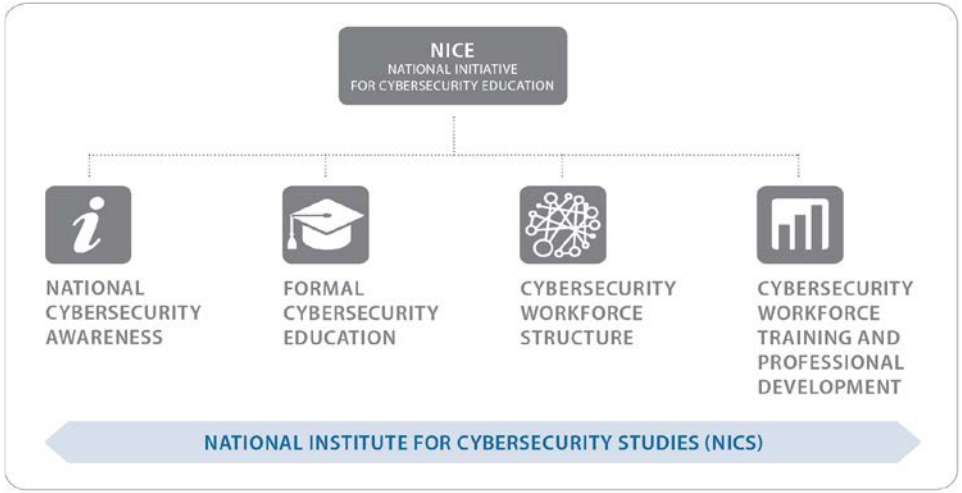
- **Open Sourcing**
- **Licensing**
- **New Companies**
- **Adoption by cyber operations analysts**
- **Direct private-sector adoption**
- **Government use**

❑ Implement Presidential Memorandum – "Accelerating Technology Transfer and Commercialization of Federal Research in Support of High-Growth Businesses" (Oct 28, 2011)

A National Problem

- The Nation needs greater cybersecurity awareness and more cybersecurity experts.
- There is a lack of communication between government, private industry, and academia.
- Many cybersecurity training programs exist but there is little consistency among programs, and potential employees lack information about the skills needed for jobs.
- Cybersecurity Career development and scholarships are available but uncoordinated, and the resources that do exist are difficult to find.

NICE was established in support of the Comprehensive National Cybersecurity Initiative (CNCI) – Initiative 8: Expand Cyber Education – Interim Way Forward and is comprised of over 20 federal departments and agencies.



Cybersecurity Education

- Cyber Security Competitions **(http://nationalccdc.org)**
  - National Initiative for Cybersecurity Education (NICE)
  - NCCDC (Collegiate); U.S. Cyber Challenge (High School)
    - Provide a controlled, competitive environment to assess a student's depth of understanding and operational competency in managing the challenges inherent in protecting a corporate network infrastructure and business information systems.

- DHS Cyber Skills Task Force (CSTF)
  - Established June 6, 2012 - Homeland Security Advisory Council
  - Over 50 interviews (DHS internal and external)
    - Identify best ways DHS can foster the development of a national security workforce capable of meeting current and future cybersecurity challenges;
    - Outline how DHS can improve its capability to recruit and retain sophisticated cybersecurity talent.
  - 11 recommendations in 5 key areas

DHS Cyber Skills Task Force (CSTF) - Objectives

- **Objective I:** **Ensure that the people given responsibility for mission-critical cybersecurity roles and tasks at DHS have demonstrated that they have high proficiency in those areas.**

- **Objective II:** **Help DHS employees develop and maintain advanced technical cybersecurity skills and render their working environment so supportive that qualified candidates will prefer to work at DHS.**

- **Objective III:** **Radically expand the pipeline of highly qualified candidates for technical mission-critical jobs through partnerships with community colleges, universities, organizers of cyber competitions, and other federal agencies.**

- **Objective IV:** **Focus the large majority of DHS's near term efforts in cybersecurity hiring, training, and human capital development on ensuring that the Department builds a team of approximately 600 federal employees with mission-critical cybersecurity skills.**

- **Objective V:** **Establish a "CyberReserve" program to ensure a cadre of technically proficient cybersecurity professionals are ready to be called upon if and when the nation needs them.**

Homeland Security

Homeland Security
Science and Technology

White House Priorities – FY14+

- Secure Federal Networks
  - ICAM, Cloud Exchange, Fed-CERT
- Protect Critical Infrastructure
  - Public-Private Cyber Coordination, EO/PPD Initiatives
- Improve Incident Response and Reporting
  - Information Sharing among Federal Centers
  - Capacity Building for SLTTs
- Engage Internationally
  - Foreign Assistance Capacity Building
  - Build Workforce Capacity to Support International Cyber Engagement
- Shape the Future
  - National Strategy for Trusted Identity in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)
  - Cybersecurity R&D – EO/PPD R&D Plan, Federal R&D Plan, Transition To Practice, Foundational Research

DHS S&T CSD Budgets

- Cybersecurity Research Infrastructure - $7.3M
- Software Assurance - $7.6M
- Network Security - $9.1M
- Mobile, Web, and Cloud Security - $2.2M
- Identity Management and Privacy - $5.0M
- Usability and Metrics - $4.5M
- Cyber Security Education and Training - $2.3M
- CNCI - $17.3M
- Securing Critical Infrastructure - $9.9M
- Law Enforcement Needs - $9.0M

- Total - $74.2M

CSD New Starts – FY13-14

- Security for Cloud-Based Systems
  - Ed Rhyne
- Data Privacy Technologies
  - Karyn Higa-Smith
- Mobile Wireless Investigations
  - Megan Mahle
- Mobile Device Security
  - Luke Berndt
  - Collaboration Session on Tuesday

Other CSD Program Ideas

- Next-Generation DDOS Defenses
  - Dan Massey
- Cyber-Physical Systems
  - Dan Massey
- Application Security Threat Attack Modeling (ASTAM)
  - Kevin Greene
- Static Tool Analysis Modernization Project (STAMP)
  - Kevin Greene
- Network Reputation and Risk Analysis
  - Manish Karir, Ann Cox
- Data Analytics Methods for Cyber Security
  - Joe Kielman
- Cyber Security Education
  - Scott Tousley
- Designed-In Security - TBD
- Finance Sector Cybersecurity - TBD

Homeland Security
Science and Technology

Summary

- Cybersecurity research is a key area of innovation to support our global economic and national security futures
- DHS S&T continues with an aggressive cyber security research agenda
  - Working to solve the cyber security problems of our current (and future) infrastructure and systems
  - Working with academe and industry to improve research tools and datasets
  - Looking at future R&D agendas with the most impact for the nation
- Need to continue strong emphasis on technology transfer and experimental deployments
- Must focus on the education, training, and awareness aspects of our current and future cybersecurity workforce

Homeland Security
Science and Technology

Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170

For more information, visit

http://www.cyber.st.dhs.gov

http://www.dhs.gov/cyber-research

Homeland Security

Science and Technology

PI Meeting Planning Comm.

- Jean Camp, Univ of Indiana
- KC Claffy, UC San Diego
- Anita D'Amico, Secure Decisions
- John Goodall, Oak Ridge National Lab
- Dimitris Pendarakis, IBM
- Kathryn Perrett, Canada DRDC
- Ann Cox, Kevin Greene, Joe Kielman – CSD PMs
- Melissa Ho, Shelby Smith, Kyshina Chandler, Michael Reagan – CSD Support Staff

PM / PI Financial Guidance - 1

- **FY13 has been an incredible year – Budget / Contracting**
- Due to the FY13 continuing resolution and sequestration, CSD did not get its final budget until May 24th.
- With a condensed budget execution schedule and overwhelming number of funding documents, our CFO has had issues sending FY13 funds to AFRL and SSC-PAC.
- For those of you still waiting for your FY13 funds, please be patient. AFRL should have money in October. SSC-PAC will likely be November or December.
- We realize this has already caused some of you issues and we're doing everything we can to send your funds.

PM / PI Financial Guidance - 2

- 52.232-22 - Limitation of Funds - 75 percent notice
  LIMITATION OF FUNDS (APR 1984)
- (c) The Contractor shall notify the Contracting Officer in writing whenever it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the contract by the Government or, (2) if this is a cost-sharing contract, the amount then allotted to the contract by the Government plus the Contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the Schedule.
- **IF YOU HAVEN’T DONE THIS, THEN PLEASE DO SO!!**

PM / PI Financial Guidance - 3

- 5252.232-9210 LIMITATION OF LIABILITY--INCREMENTAL FUNDING (JAN 1992)
- This contract is incrementally funded and the amount currently available for payment hereunder is limited to <your contract value>. It is estimated that these funds will cover the cost of performance through <POP – incremental>. Subject to the provisions of the FAR 52.232-22 "Limitation of Funds" clause of this contract, no legal liability on the part of the Government for payment in excess of <your contract value> shall arise unless additional funds are made available and are incorporated as modifications to this contract. The total remaining unfunded amount is <some amount>.
- What that means is: **PERFORMERS CANNOT SPEND WHAT THEY DO NOT HAVE**

PM / PI Financial Guidance - 4

- **Bottom Line:**
- Performers MUST avoid unauthorized commitments
- PIs MUST know what has been INVOICED and what still needs to be invoiced
- PIs must know if subcontractors have been billing or NOT
- PMs must ensure performers do not work if they are out of funds! No overruns.
- Government NEVER encourages Working at Risk
- Working at Risk is a discussion/decision made ONLY by the performer. Future payment by the Government is NEVER guaranteed.

Guidance for PI Presentations

- The allotted briefing times are as follows: 15 minutes per PI plus 5 minute Q&A (new contracts are 10 minutes)
- Slide Formats - Use Presentation Format provided
  - NABC Format – Customer Need, Approach, Benefit, Competition
- Confidence Monitor
- **NO** questions during presentations
  - Save them for the end or talk during the breaks

PI Meeting Expectations

- Rule #1: Expect all to participate, ask questions, provide feedback (both online and offline – use tact)
- Rule #2: Take opportunities to talk with others about collaborative opportunities
  - Seven international partners (AUS, CA, DE, EU, NL, SW, UK) are present. Some have already co-funded projects and others are interested in possibly co-funding future work
  - Especially interested in identifying possible experiments with integration of multiple technologies
- Rule #3: Comments/Critique of agenda
  - Planning Committee did an excellent job. Trying many new things this year with webcasting, collaboration sessions, mini-PI meetings, etc.
  - **ACTION:** If you have other ideas for format, content, etc., please let us know.

Administrative Information

- PR – Public Relations and/or Press Releases
  - Anytime you have something that appears in the press, please coordinate with your PM and SETA. If you mention DHS S&T (which you should), then we need to see it.
  - Pre-publication review – Anytime you will be presenting or publishing a paper, please send it to your PM and SETA in advance for review and clearance. If you are receiving international co-funding, you need to factor even more time for pre-pub review. Coordinate with your PM and SETA.