THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

SUPPLEMENT TO THE PRESIDENT'S BUDGET

FY 2016

FEBRUARY 2015

Networking and Information Technology Research and Development
National Coordination Office

George O. Strawn
Director

Mark A. Luker
Deputy Director

Margaret E. Harmsen
Editor, FY 2016 NITRD Budget Supplement

Diane R. Theiss
Budget Analyst

4201 Wilson Boulevard, Suite II-405
Arlington, Virginia 22230
(703) 292-4873
nco@nitrd.gov

Acknowledgments

This Supplement to the President's Budget was developed through the contributions of the NITRD Federal agency representatives and members, the NCO staff, and other Federal agencies participating in the NITRD Program. We extend our sincere thanks and appreciation to all who have contributed.

National Coordination Office for Networking and Information Technology Research and Development

The annual NITRD Supplement to the President's Budget is prepared and published by the National Coordination Office for Networking and Information Technology Research and Development (NITRD/NCO). The NCO staff coordinates the activities of the NITRD Program and supports overall planning, budget, and assessment activities for the multiagency NITRD enterprise under the auspices of the NITRD Subcommittee of the National Science and Technology Council's (NSTC) Committee on Technology (CoT).

About the Document

This document is a supplement to the President's Fiscal Year 2016 Budget Request. It describes the activities underway in 2015 and planned for 2016 by the Federal agencies participating in the NITRD Program, primarily from a programmatic and budgetary perspective. It reports actual investments for FY 2014 and requested investments for FY 2016 by Program Component Area (PCA). It identifies the NITRD Program's strategic priorities by PCA for budgetary requests; strategic priorities underlying the requests; highlights of the requests; planning and coordination activities supporting the request; and 2015 and 2016 activities by agency.

Digital versions of NITRD documents are available on the NITRD website: *www.nitrd.gov*.

SUPPLEMENT TO THE PRESIDENT'S BUDGET
FOR FISCAL YEAR 2016

THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

A Report by the
Subcommittee on Networking and Information Technology
Research and Development

Committee on Technology
National Science and Technology Council

FEBRUARY 2015

National Science and Technology Council Committee on Technology

Thomas Kalil, Chair, OSTP
Jayne B. Morrow, Executive Secretary (Acting), OSTP

Subcommittee on Networking and Information Technology Research and Development

Co-Chairs
James F. Kurose, NSF
George O. Strawn, NCO

Department of Commerce

NIST
Representative
Charles H. Romine
Alternate
Kamie Roberts

NOAA
Representative
David L. Michaud
Alternate
Darren L. Smith

Department of Defense

DARPA
Representative
Daniel Kaufman

NSA
Representative
Christopher D. Green
Alternate
Candace S. Culhane

OSD
Representative
Steven E. King
Alternate
Dai H. Kim

SERVICE RESEARCH ORGANIZATIONS:

Air Force
Representative
Russell Partch

Army
Representative
Mary J. Miller
Alternate
Karen L. O'Conner

Navy
Representative
Sukarno Mertoguno

Department of Energy

DOE/NNSA
Representative
Robert Meisner
Alternate
Thuc T. Hoang

DOE/OE
Representative
Carol Hawk

DOE/SC
Representative
J. Steve Binkley
Alternates
William Harrod
Barbara Helland

Department of Health and Human Services

AHRQ
Representative
Gurvaneet Randhawa

NIH
Representative
Susan Gregurick
Alternate
Peter M. Lyster

ONC
Representative
Vacant

Department of Homeland Security

DHS
Representative
Douglas Maughan
Alternate
Luke Berndt

Independent Agencies

EPA
Representative
Gary L. Walter

NASA
Representative
Bryan A. Biegel

NARA
Representative
Mark Conrad

NRO
Representative
Robert Jimenez
Alternate
Richard D. Ridgley

NSF
Representative
James F. Kurose
Alternate
C. Suzanne Iacono

OMB
Representative
Tali Bar-Shalom

OSTP
Representative
Nick Maynard

NITRD/NCO
Representative
George O. Strawn
Alternate
Mark A. Luker

Executive Secretary
Nekeia Butler

EXECUTIVE OFFICE OF THE PRESIDENT
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
WASHINGTON, D.C. 20502

February 24, 2015

Members of Congress:

I am pleased to transmit the FY 2016 annual report of the Federal Government's multi-agency Networking and Information Technology Research and Development (NITRD) Program. This Program, which today comprises 20 member agencies and many additional participating agencies, coordinates Federal research and development investments in advanced digital technologies that are essential to the Nation's economic growth and prosperity. NITRD agencies work closely together in the planning and execution of their respective research programs, enabling the Program as a whole to leverage investments in ways that have a greater positive impact than agencies could achieve working alone.

Advances in digital technologies have helped stimulate economic growth, innovation, and job creation in the United States and have revolutionized capabilities central to business, government, and education around the world. Continued progress in the development of networking and information technologies will drive further advances in the sciences, national security, manufacturing, health, energy, education, transportation, and the environment.

President Obama has emphasized that networking and computing capabilities will also be foundational to advancing several key priorities for his Administration, including expanding the frontiers of knowledge about the human brain; advancing the development of medical treatments that are more precisely tailored to individuals; developing sustainable energy sources and energy delivery systems; and ensuring an open and free Internet that is secure, resilient, and affords appropriate privacy protections.

Federal NITRD investments made today will be crucial to the creation of tomorrow's new industries and workforce opportunities. I look forward to continuing to work with you to support this vital Federal program.

Sincerely,

John P. Holdren
Assistant to the President for Science and Technology
Director, Office of Science and Technology Policy

Contents

NITRD Member Agencies

The following Federal agencies conduct or support R&D in advanced networking and information technologies, report their IT research budgets in the NITRD crosscut, and provide support for program coordination:

Department of Commerce (DOC)
- National Institute of Standards and Technology (NIST)
- National Oceanic and Atmospheric Administration (NOAA)

Department of Defense (DoD)
- Defense Advanced Research Projects Agency (DARPA)
- National Security Agency (NSA)
- Office of the Secretary of Defense (OSD)
- Service Research Organizations (Air Force, Army, Navy)

Department of Energy (DOE)
- National Nuclear Security Administration (DOE/NNSA)
- Office of Electricity Delivery and Energy Reliability (DOE/OE)
- Office of Science (DOE/SC)

Department of Health and Human Services (HHS)
- Agency for Healthcare Research and Quality (AHRQ)
- National Institutes of Health (NIH)
- Office of the National Coordinator for Health Information Technology (ONC)

Department of Homeland Security (DHS)
Environmental Protection Agency (EPA)
National Aeronautics and Space Administration (NASA)
National Archives and Records Administration (NARA)
National Reconnaissance Office (NRO)
National Science Foundation (NSF)

NITRD Participating Agencies

The following Federal agencies participate in NITRD activities and have mission interests that involve applications and R&D in advanced networking and information technologies:

Department of Commerce (DOC)
- National Telecommunications and Information Administration (NTIA)

Department of Defense (DoD)
- Military Health System (MHS)
- Telemedicine and Advanced Technology Research Center (TATRC)

Department of Education (ED)
Department of Health and Human Services (HHS)
- Centers for Disease Control and Prevention (CDC)
- Food and Drug Administration (FDA)
- Indian Health Service (IHS)

Department of Interior (Interior)
- U.S. Geological Survey (USGS)

Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- National Institute of Justice (NIJ)

Department of Labor (DOL)
- Bureau of Labor Statistics (BLS)

Department of State (State)
Department of Transportation (DOT)
- Federal Aviation Administration (FAA)
- Federal Highway Administration (FHWA)

Department of the Treasury (Treasury)
- Office of Financial Research (OFR)

Department of Veterans Affairs (VA)
Federal Communications Commission (FCC)
Federal Deposit Insurance Corporation (FDIC)
General Services Administration (GSA)
Nuclear Regulatory Commission (NRC)
Office of the Director of National Intelligence (ODNI)
- Intelligence Advanced Research Projects Activity (IARPA)

U.S. Agency for International Development (USAID)
U.S. Department of Agriculture (USDA)
- National Institute of Food and Agriculture (NIFA)

Introduction and Overview

The Networking and Information Technology Research and Development (NITRD) Program is the Nation's primary source of federally funded work on advanced information technologies in computing, networking, and software. Through its interagency coordination and collaboration activities, the NITRD Program seeks to provide the research and development foundations for the advanced information technologies that sustain U.S. technological leadership and meet the needs of the Federal Government. The NITRD Program also seeks to accelerate the development and deployment of advanced information technologies that enable world-class science and engineering, enhance national defense and homeland security, improve U.S. productivity and economic competitiveness, protect the environment, and improve the health, education, and quality of life of all Americans.

Highlights of NITRD Program developments over the past year include:

- *Big Data:* The focus of the Big Data Senior Steering Group (BD SSG) turned to strategic planning, with activities currently in progress across agencies and with the public to solicit broad inputs to the development of a Federal Big Data Research Agenda, proposed for 2015.
- *Cyber-Physical Systems*: The joint solicitation for foundational research in cyber-physical systems (CPS) expanded in FY 2014 to include NSF, DHS, and DOT, demonstrating successful interagency collaborations. The Cyber Physical Systems Senior Steering Group (CPS SSG) also collaborated with experts from the White House Presidential Innovation Fellows program on the SmartAmerica and Global City Teams Challenges. These projects are spurring innovation in CPS and the Internet of Things (IoT) through public-private partnerships.
- *Cybersecurity and Privacy R&D*: NITRD agencies continued to give cybersecurity R&D a priority focus and to support programs and activities that align with the Federal Cybersecurity R&D Strategic Plan.[1] The agencies are currently reviewing the recently passed Cybersecurity Enhancement Act of 2014 to determine next steps and actions. At the Office of Science and Technology Policy's (OSTP) request this past summer, the Cybersecurity R&D SSG is leading an effort to develop a National Privacy Research Strategy, with activities underway to define a privacy research framework. The tasking follows reports by the White House and the President's Council of Advisors on Science and Technology (PCAST) on big data and privacy,[2,3] and PCAST's recommendations to NITRD on developing the science and engineering foundations for privacy R&D.[4]
- *High-End Computing*: NITRD agencies continued to support high-end computing programs and activities that align with the *Federal Plan for High-End Computing*[5] while coordinating with the Administration on the development of a future national-level computing strategy.
- *Video and Image Analytics Coordinating Group*: The NITRD Program recently welcomed the Video and Image Analytics Coordinating Group (VIA CG), a new interagency coordination group focused on video and image analytics of the visible world. The VIA CG grew from an affiliation of Federal agencies that came together in the aftermath of the 2013 Boston Marathon attacks to address the challenges of video analysis across a variety of domains such as communications, defense, energy, law enforcement, space, and transportation.

---

[1] *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,* December 2011, NSTC: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[2] *Big Data: Seizing Opportunities, Preserving Values*. May 2014, Executive Office of the President: http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
[3] *Big Data and Privacy: A Technological Perspective*. May 2014, PCAST: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf
[4] *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*. January 2013, PCAST: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf
[5] *Federal Plan for High-End Computing*. May 2004, NSTC High-End Computing Revitalization Task Force: https://www.nitrd.gov/pubs/2004_hecrtf/20040510_hecrtf.pdf

- *Wireless Spectrum-Sharing*: Through a series of workshops, the Wireless Spectrum R&D SSG continued to make progress in highlighting efforts to increase spectrum sharing between government and private sectors, gather research information, build collaboration, and advance spectrum-sharing technology innovation.

About the NITRD Program

Now in its 24th year, the NITRD Program is one of the oldest and largest of the formal Federal programs that engage multiple agencies in support of the Federal Government's mission of sponsoring and investing in fundamental research and development. As required by the High-Performance Computing Act of 1991 (P.L. 102-194), the Next Generation Internet Research Act of 1998 (P.L. 105-305), and the America COMPETES (Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science) Act of 2007 (P.L. 110-69), the NITRD Program provides a framework and mechanisms for coordination among the Federal agencies that support advanced information technology (IT) R&D and report IT research budgets in the NITRD crosscut. Many other agencies with IT interests also participate in NITRD activities.

Agencies coordinate their NITRD research activities and plans in eight Program Component Areas (PCAs), which are the major subject areas under which related projects and activities carried out under the NITRD Program are grouped. Budgets for the PCAs are reported in the annual NITRD budget crosscut. The PCAs are:

- Cybersecurity and Information Assurance (CSIA)
- High Confidence Software and Systems (HCSS)
- High End Computing Infrastructure and Applications (HEC I&A)
- High End Computing Research and Development (HEC R&D)
- Human Computer Interaction and Information Management (HCI&IM)
- Large Scale Networking (LSN)
- Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)
- Software Design and Productivity (SDP)

For each PCA, agency representatives meet in an Interagency Working Group (IWG) or a Coordinating Group (CG) to exchange information and collaborate on research plans and activities such as testbeds, workshops, and cooperative solicitations. Such activities enable agencies to coordinate and focus their R&D resources on important, shared problems with the common goals of making new discoveries and/or developing new technological solutions. For example, IT testbeds provide structured environments, akin to laboratory workbenches, where researchers test hypotheses, perform measurements, and collaborate under conditions similar to real-world environments. For agencies, the economic and engineering benefits of sharing IT testbed environments can be substantial, including avoiding the expense of duplicate facilities. Additional benefits accrue from cultivating a vibrant scientific and intellectual enterprise in which researchers across various agencies, disciplines, and sectors share ideas and results, speeding the overall pace of innovation.

The NITRD coordinating structure also includes Senior Steering Groups (SSGs) to focus on emerging science and technology priorities. The SSGs enable senior-level individuals who have the authority to affect or shape the R&D directions of their organizations to collaborate on developing effective R&D strategies for national-level IT challenges. The program focus areas coordinated by SSGs include:

- Big Data (BD)
- Cyber Physical Systems (CPS)
- Cybersecurity and Information Assurance Research and Development (CSIA R&D)

- Wireless Spectrum Research and Development (WSRD)

The NITRD Program also supports Communities of Practice (CoPs) that function as forums to enhance R&D collaboration and promote the adoption of advanced IT capabilities developed by government-sponsored IT research. The CoPs are:

- Faster Administration of Science and Technology Education and Research (FASTER)
- Health Information Technology Research and Development (HITRD)

Overall NITRD Program coordination is carried out by the Subcommittee on Networking and Information Technology Research and Development, under the aegis of the Committee on Technology (CoT) of the National Science and Technology Council (NSTC). The NITRD Subcommittee convenes three times a year and the IWGs, CGs, SSGs, and CoPs each meet approximately 12 times annually. The NITRD National Coordination Office (NITRD/NCO) provides technical, administrative, and logistical support for the activities of the NITRD Program, including publication of the annual NITRD Supplement to the President's Budget.

For further information about the NITRD Program, please see the NITRD website: www.nitrd.gov.

About the NITRD Supplement to the President's Budget

The annual Supplement to the President's Budget for the NITRD Program provides a technical summary of the research activities planned and coordinated through NITRD in a given Federal budget cycle, as required by law. The details are organized by PCA and presented using a common format:

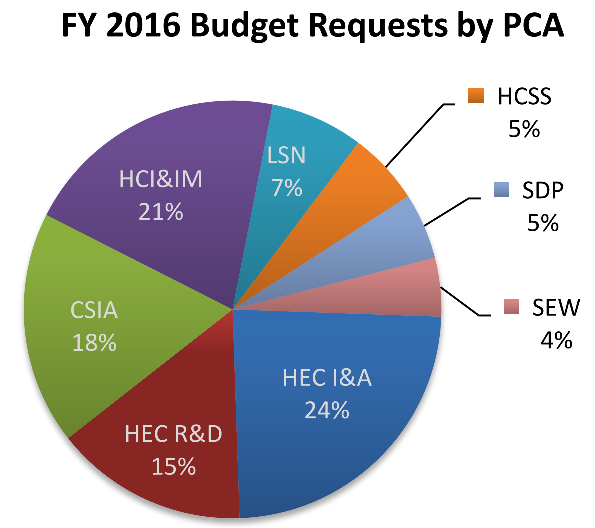
- Listing of the NITRD member agencies and participating agencies active in the PCA
- Definition of the research covered in the PCA
- Strategic priorities in the PCA for the forthcoming fiscal year
- Budget highlights – agencies' key R&D programs and topical emphases in the PCA for the forthcoming year
- Interagency coordination – current and planned activities in which multiple agencies are collaborating
- Ongoing core activities of each agency in the PCA

The NITRD Supplement includes an annual budget table and budget analysis section, organized by PCA and by agency, to facilitate budgetary and programmatic comparisons from year to year.

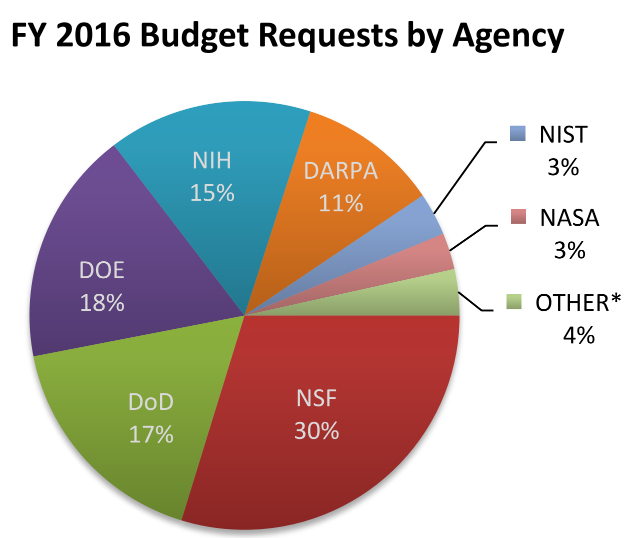
In addition, the NITRD Supplement provides brief summaries of the interagency program focus areas coordinated under the NITRD Program's SSGs and CoPs, including each group's strategic priorities and current and planned coordination activities for the forthcoming year.

The President's FY 2016 budget request for the NITRD Program is $4.1 billion, while the FY 2015 estimate totaled $4.0 billion. Details of the budget are presented in the table on pages 6-7 and discussed in the budget analysis section.

The following illustration shows the percentages of the FY 2016 budget requests by PCA.[6]



The following illustration shows the percentages of the FY 2016 budget requests by agency.[7]

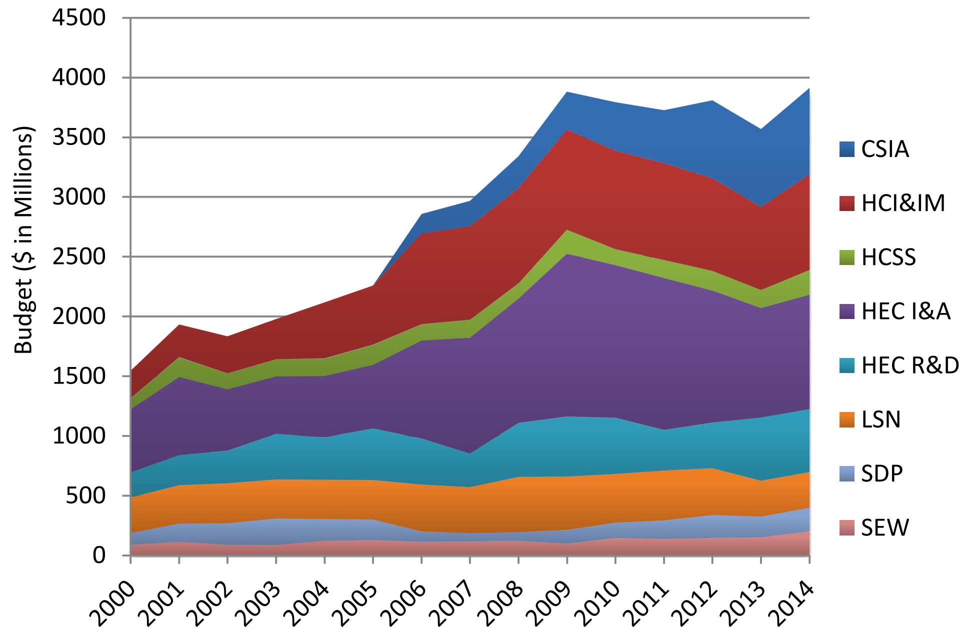


*Includes AHRQ, DHS, EPA, NARA, and NOAA.

[6] Totals may not sum correctly due to rounding.
[7] Same as footnote 6.

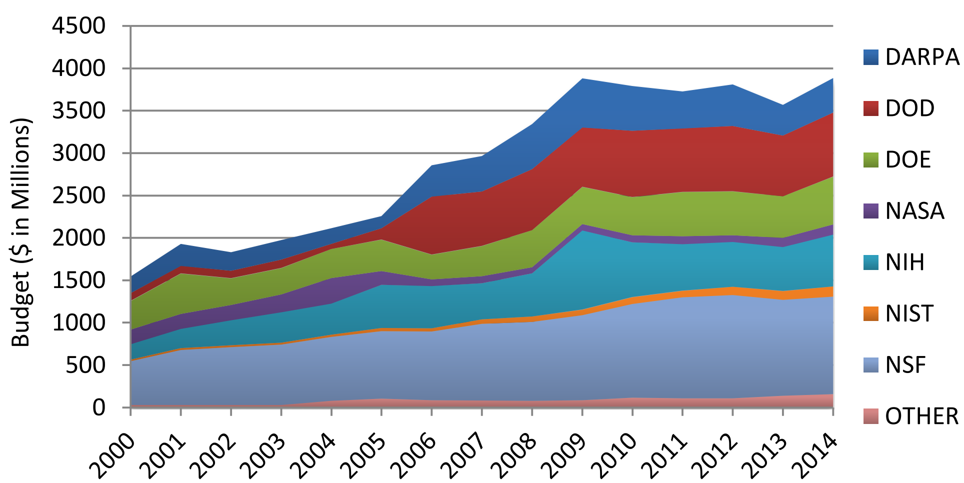
The following illustration shows budget trends by PCA since FY 2000.[8]

Budget Trends by PCA



The following illustration shows budget trends by agency since FY 2000.[9]

Budget Trends by Agency



DOD includes OSD and DoD Service research organizations. DOE includes DOE/NNSA, DOE/OE, and DOE/SC. OTHER includes AHRQ, DHS, EPA, NARA, and NOAA.

[8] The budget trends illustrations use budget estimates for FY 2000 - FY 2009 and budget actuals for FY 2010 and beyond.
[9] Same as footnote 8.

Agency NITRD Budgets by Program Component Area

Key: FY 2014 Budget Actuals, *FY 2015 Budget Estimates*, and **FY 2016 Budget Requests**
(Dollars in Millions)

Agency/ Program Component Area		Cybersecurity & Information Assurance (CSIA)	High Confidence Software & Systems (HCSS)	High End Computing Infrastructure & Applications (HEC I&A)	High End Computing Research & Development (HEC R&D)	Human Computer Interaction & Information Management (HCI&IM)	Large Scale Networking (LSN)	Social, Economic, & Workforce Implications of IT (SEW)	Software Design & Productivity (SDP)	Total[10]
	FY 2014 Actual	103.4	87.2	233.6	116.0	282.6	131.7	119.8	77.6	1,151.8
	FY 2015 Estimate	*106.8*	*94.9*	*217.9*	*131.8*	*292.3*	*127.9*	*125.8*	*88.6*	*1,186.0*
NSF	**FY 2016 Request**	**111.7**	**97.9**	**221.4**	**138.4**	**297.0**	**130.8**	**129.1**	**90.6**	**1,217.0**
		182.5	56.4	82.0	240.3	98.7	80.5	0.4	14.2	755.0
		152.1	*37.5*	*73.4*	*243.3*	*136.2*	*63.4*		*7.6*	*713.4*
DoD[11]		**156.1**	**53.0**	**78.9**	**204.2**	**132.8**	**66.8**	**2.7**	**8.7**	**703.4**
		30.7	7.5	333.6	107.1		58.4	8.7		546.0
		32.7	*25.0*	*374.7*	*128.1*		*71.6*	*3.0*		*635.1*
DOE[12]		**30.0**	**15.0**	**352.3**	**214.6**		**78.2**	**10.0**		**700.2**
		1.0	24.0	190.0	17.0	251.1	6.0	31.0	92.0	612.0
		1.0	*24.0*	*191.0*	*17.0*	*250.0*	*6.0*	*31.0*	*93.0*	*613.0*
NIH		**1.0**	**25.0**	**196.0**	**18.0**	**255.0**	**6.0**	**32.0**	**95.0**	**628.0**
		265.3	4.5		35.1	96.1	7.5			408.5
		309.3	*8.0*		*26.5*	*75.5*				*419.2*
DARPA		**297.7**	**12.1**		**23.2**	**100.0**				**433.0**
		61.6	13.9	14.4	3.1	10.1	7.9	4.4	4.1	119.5
		67.6	*13.9*	*14.4*	*3.1*	*10.1*	*7.9*	*4.4*	*4.1*	*125.5*
NIST		**72.6**	**14.9**	**14.4**	**3.1**	**11.1**	**7.9**	**4.4**	**4.1**	**132.5**
			13.5	73.2	0.8	20.5	1.0		10.5	119.5
			10.5	*67.3*	*1.1*	*20.5*	*1.0*		*10.1*	*110.5*
NASA			**9.8**	**69.1**	**1.1**	**20.5**	**1.0**		**10.6**	**112.1**
		77.8				10.0		3.8		91.6
		67.5				*7.2*		*4.4*		*79.1*
DHS[13]		**69.0**						**4.0**		**73.0**
				21.4	0.2	1.5	3.3		0.7	27.1
				24.5	*0.2*	*1.5*	*3.3*		*0.7*	*30.2*
NOAA				**33.5**	**0.2**	**1.5**	**3.3**		**0.7**	**39.2**
						29.1	0.5			29.6
						27.7	*0.5*			*28.2*
AHRQ						**22.4**	**0.5**			**22.9**
				9.0	5.0			3.0		17.0
				8.9	*7.8*			*2.7*		*19.4*
DOE/ NNSA				**9.6**	**9.1**			**3.5**		**22.2**

[10] Totals may not sum correctly due to rounding.

[11] DoD budget includes funding for OSD and the DoD Service research organizations. DoD Service research organizations include: Air Force Research Laboratory (AFRL), including the Air Force Office of Scientific Research (AFOSR); Army Research Laboratory (ARL), including the Army Research Office (ARO); Naval Research Laboratory (NRL); and Office of Naval Research (ONR). The Communications-Electronics Research, Development, and Engineering Center (CERDEC), Defense Research and Engineering Network (DREN), and High Performance Computing Modernization Program (HPCMP) are under Army. Although DARPA and OSD research organizations are under DoD, they are independent of the research organizations of the DoD Services (Air Force, Army, and Navy). NSA is a research organization under DoD, but does not report NITRD funding.

[12] DOE budget includes funding from DOE's Office of Science (SC), Office of Electricity Delivery and Energy Reliability (OE), and Energy Transformation Acceleration Fund.

[13] As of the date the 2016 Budget was released, final 2015 appropriations for DHS were not yet enacted. Therefore, the 2015 row of this table reflects amounts requested for DHS in the 2015 Budget.

Agency/ Program Component Area		Cybersecurity & Information Assurance (CSIA)	High Confidence Software & Systems (HCSS)	High End Computing Infrastructure & Applications (HEC I&A)	High End Computing Research & Development (HEC R&D)	Human Computer Interaction & Information Management (HCI&IM)	Large Scale Networking (LSN)	Social, Economic, & Workforce Implications of IT (SEW)	Software Design & Productivity (SDP)	Total[10]
EPA	FY 2014 Actual			3.3		3.0				6.3
	FY 2015 Estimate			*3.2*		*2.7*				*5.9*
	FY 2016 Request			**3.0**		**2.5**				**5.5**
DOT[14]			1.5							1.5
			1.5							*1.5*
			1.5							**1.5**
NARA						0.2				0.2
						0.2				*0.2*
						0.2				**0.2**
Total FY 2014 Actuals[10]		722.3	208.4	960.5	524.6	802.9	296.8	171.1	199.1	3,885.6
Total FY 2015 Estimates[10]		*736.9*	*215.3*	*975.3*	*558.8*	*823.9*	*281.6*	*171.2*	*204.1*	*3,967.1*
Total FY 2016 Requests[10]		**738.2**	**229.3**	**978.2**	**611.9**	**842.9**	**294.6**	**185.7**	**209.8**	**4,090.6**

NITRD Program Budget Analysis

Fiscal Year Overview for 2015-2016

In the following analysis of the NITRD Program, the President's FY 2016 request is compared with the FY 2015 estimates. Changes in NITRD Program budgets reported in the budget analysis reflect revisions to program budgets due to evolving priorities, as well as Congressional actions and appropriations.

Summary

The President's 2016 budget request for the NITRD Program is $4.1 billion, an increase of $100 million, approximately 2.5 percent more than the $4.0 billion 2015 estimate. The overall change is due to both increases and decreases in individual agency NITRD budgets, which are described below.

NITRD Program Budget Analysis by Agency

This section describes changes greater than $10 million between 2015 estimated spending and 2016 requests. Smaller changes are discussed only if they represent shifts in funding focus. Budget numbers in these descriptions are rounded from initial agency numbers with three decimals to the nearest tenth.

NSF

Comparison of 2015 estimate ($1,186.0 million) and 2016 request ($1,217.0 million): The $31.0 million increase is primarily due to increases of $6.6 million in HEC R&D for Advanced Computational Infrastructure; $4.9 million in CSIA for Secure and Trustworthy Cyberspace (SaTC) and Innovations at the Nexus of Food, Energy, and Water Systems (INFEWS); and $4.7 million in HCI&IM for Cyber-enabled Materials, Manufacturing, and Smart Systems (CEMMSS) and Understanding the Brain, with smaller increases in other PCAs.

DoD

Comparison of 2015 estimate ($713.4 million) and 2016 request ($703.4 million): The decrease of $10.0 million is primarily due to a $39.1 million decrease in HEC R&D following higher FY 2015 estimated spending enabled by the additional funds appropriated by Congress for the High Performance Computing Modernization Program (HPCMP) for FY 2015, with smaller increases and decreases in other PCAs, partially offset by an increase of $15.5 million in HCSS.

[14] DOT budget is included to reflect funding for transportation initiatives beginning in FY 2014.

DOE

Comparison of 2015 estimate ($635.1 million) and 2016 request ($700.2 million): The $65.1 million increase is primarily due to an $86.5 million increase in DOE/SC funding in HEC R&D for exascale computing, with smaller increases in other PCAs, partially offset by a decrease of $22.4 million in HEC I&A due to the completion of some site preparations for planned upgrades at the Leadership Computing Facilities and other program shifts, and a decrease of $10.0 million in HCSS following higher FY 2015 estimated spending on the additional projects expected under the ARPA-E Open 2015 Funding Opportunity Announcement.

NIH

Comparison of 2015 estimate ($613.0 million) and 2016 request ($628.0 million): The increase of $15.0 million is primarily due to increases of $5.0 million in HEC I&A for the development of high end computing applications to support innovative biomedical research and $5.0 million in HCI&IM for new information management programs, with smaller increases in other PCAs.

DARPA

Comparison of 2015 estimate ($419.2 million) and 2016 request ($433.0 million): The increase of $13.8 million is primarily due to a $24.5 million increase in HCI&IM for enhanced language translation efforts and an increase for the Big Mechanism program, with smaller increases and decreases in other PCAs, partially offset by a decrease of $11.6 million in CSIA due to the completion of the Rapid Software Development using Binary Components (RAPID) and Crowd Sourced Formal Verification (CSFV) programs, and the drawdown of several cyber programs: Automated Program Analysis for Cybersecurity (APAC), Plan X, and Cyber Grand Challenge.

NITRD Program Budget Analysis by PCA

Using the information presented above, this section provides an analysis of the NITRD Program budget by PCA, summarizing the more substantial differences between 2015 estimates and 2016 requests. The changes are described below.

HCSS

Comparison of 2015 estimate ($215.3 million) and 2016 request ($229.3 million): The $14.0 million increase is largely due to an increase of $15.5 million at DoD, with smaller increases and decreases at other agencies, partially offset by a $10.0 million decrease at DOE.

HEC R&D

Comparison of 2015 estimate ($558.8 million) and 2016 request ($611.9 million): The $53.1 million increase is largely due to an increase of $86.5 million at DOE, with smaller increases and decreases at other agencies, partially offset by a $39.1 million decrease at DoD.

HCI&IM

Comparison of 2015 estimate ($823.9 million) and 2016 request ($842.9 million): The $19.0 million increase is largely due to an increase of $24.5 million at DARPA, with smaller increases and decreases at other agencies.

LSN

Comparison of 2015 estimate ($281.6 million) and 2016 request ($294.6 million): The $13.0 million increase is largely due to an increase of $6.6 million at DOE for the Energy Sciences network (ESnet) and for Small Business Innovation Research (SBIR), with smaller increases and decreases at other agencies.

SEW

Comparison of 2015 estimate ($171.2 million) and 2016 request ($185.7 million): The $14.5 million increase is largely due to an increase of $7.0 million at DOE for the Computational Sciences Graduate Fellowship, with smaller increases at other agencies.

Budget Request by Program Component Area

Cyber Security and Information Assurance (CSIA)

NITRD Agencies: AFOSR, AFRL, ARL, ARO, DARPA, DHS, DoD (CERDEC), DOE/OE, NIST, NSA, NSF, ONR, and OSD
Other Participants: DOT, IARPA, NRC, ODNI, and Treasury

CSIA focuses on research and development to detect, prevent, resist, respond to, and recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. These systems provide the IT foundation in every sector of the economy, including critical infrastructures such as power grids, financial systems, and air-traffic-control networks. These systems also support national defense, homeland security, and other Federal missions. Broad areas of emphasis include Internet and network security; security of information and computer-based systems; approaches to achieving hardware and software security; testing and assessment of computer-based systems security; reconstitution of computer-based systems and data; and resilience against cyber-attacks on computer-based systems that monitor, protect, and control critical infrastructure.

President's FY 2016 Request

Strategic Priorities Underlying This Request

High-level Federal strategic priorities for cybersecurity research are outlined in the 2011 *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*.[15] The priorities of the Strategic Plan are further refined and expanded by mission requirements of individual agencies. The role and guidance of the Strategic Plan have been reaffirmed by the OMB-OSTP Memorandum on Science and Technology Priorities for the FY 2016 Budget.[16]

The objectives for cybersecurity R&D are characterized by the following strategic directions:

- **Inducing Change** – Utilizing game-changing themes to direct efforts toward understanding the underlying root causes of known threats with the goal of disrupting the status quo; the research themes include Tailored Trustworthy Spaces, Moving Target, Cyber Economic Incentives, and Designed-In Security
- **Assuring the Mission** – Advancing cyber-supported warfighting and non-military capabilities by developing technologies to be aware of missions and threats, compute optimal assurance solutions, and implement protection as needed via mission agility or infrastructure reinforcement
- **Developing Scientific Foundations** – Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cybersecurity through adoption of a systematic, rigorous, and disciplined scientific approach
- **Maximizing Research Impact** – Catalyzing integration across the research themes, cooperation between governmental and private-sector communities, collaboration across international borders, and strengthened linkages to other national priorities, such as health and energy
- **Accelerating Transition to Practice** – Focusing efforts to ensure adoption and implementation of the new technologies and strategies that emerge from research and activities to build a scientific foundation so as to create measurable improvements in the cybersecurity landscape

[15] *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program,* December 2011, NSTC: http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf
[16] OMB-OSTP Memorandum on Science and Technology Priorities for the FY 2016 Budget (M-14-11), July 18, 2014: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-11.pdf

Highlights of Request

To address these strategic priorities, the CSIA agencies report the following topical areas as highlights of their planned R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **Inducing change**
  - **Tailored Trustworthy Spaces theme**: Enable flexible, adaptive, distributed trust environments that can support functional and policy requirements arising from a wide spectrum of user activities in the face of an evolving range of threats.
    - Cyber physical systems security – DHS, NIST, and NSF
    - Digital Provenance and Hardware-Enabled Trust Programs – DHS
    - High assurance security architectures – AFRL, DARPA, NIST, NSA, ONR, and OSD
    - IT Security Automation/Continuous Monitoring/Security Content Automation Protocol Program – DHS, NIST, and NSA
    - Operating Systems and Compilers for Heterogeneous (Multi-ISA) Computing; Rethinking Software Deployment and Customization for Improved Security and Efficiency – ONR
    - Secure wireless networking – ARL, ARO, CERDEC, DARPA, NSA, NSF, ONR, and OSD
    - Security for cloud-based systems – AFOSR, AFRL, DARPA, DHS, NIST, and NSF
    - Trusted foundation for defensive cyberspace operations – AFRL, ARL, ARO, CERDEC, ONR, and OSD
  - **Moving Target theme**: Develop capabilities to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and malicious opportunities, and increase resiliency.
    - Active Cyber Defense; Foundations of Moving Target Defense MURI – ARL
    - Agile Resilient Embedded Systems; Automated Cyber Survivability – AFRL
    - Cyber Agility Program – AFRL and OSD
    - Information Security Automation Program (ISAP) – DHS, NIST, and NSA
    - Mission-Oriented Resilient Clouds – AFRL and DARPA
    - Moving Target Defense Program – DHS
    - Proactive and Reactive Adaptive Systems – NSA
    - Robust Autonomic Computing System; Trust Management in Service Oriented Architectures – ONR
    - Security Automation and Vulnerability Management – NIST
  - **Cyber Economic Incentives theme**: Develop effective market-based, legal, regulatory, or institutional incentives to make cybersecurity ubiquitous, including incentives affecting individuals and organizations.
    - Cyber Economics Incentives Research Program – DHS
  - **Designed-in Security theme**: Develop capabilities to design and evolve high-assurance, software-intensive systems reliably while managing risk, cost, schedule, quality, and complexity. Create tools and environments that enable the simultaneous development of cyber-secure systems and the associated assurance evidence necessary to prove the system's resistance to vulnerabilities, flaws, and attacks.

    - Automated Program Analysis for Cybersecurity (APAC); High-Assurance Cyber Military Systems (HACMS) – DARPA
    - Machine Assisted Software Development; Software Development Environment for Secure System Software and Applications – ONR
    - PROgramming Computation on EncryptEd Data (PROCEED) – AFRL and DARPA
    - Roots of Trust – AFRL, NIST, and NSA
    - Software Assurance Metrics And Tool Evaluation (SAMATE) – DHS and NIST
    - Static Tool Analysis Modernization Project (STAMP) – DHS
    - Survivable Systems Engineering – OSD
    - Trusted Computing – AFRL, NSA, and OSD
  - **Cross-cutting all themes**
    - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
    - Cybersecurity for Energy Delivery Systems (CEDS) Program – DOE/OE
    - Embedded, Mobile, Tactical Systems security – OSD
- **Assuring the Mission**: Provide the ability to avoid, fight through, survive, and recover from cyber threats.
  - Application Security Threat Attack Modeling (ASTAM) – DHS
  - Assuring Effective Missions – OSD
  - Cyber-Based Mission Assurance on Trust-Enhanced Hardware (CMATH); Mission Awareness for Mission Assurance – AFRL
  - Proactive Cyber-Physical System Defense; Techniques for Robust Control Systems Design on Single- and Multi-Core Architectures – ONR
  - Resilient Cyber Defenses for Tactical Mobile – ARL
  - Resilient Infrastructure – OSD
- **Developing Scientific Foundations**
  - **Science of Security**: In anticipation of the challenges in securing the cyber systems of the future, the Federal research in the areas of science of security aims to develop an organized, scientific foundation that informs the cybersecurity domain, by organizing disparate areas of knowledge, enabling discovery of universal laws, and by applying the rigor of the scientific method.
    - Adversarial and Uncertain Reasoning for Adaptive Cyber Defense – ARO
    - Cyber measurement and experimentation – OSD
    - Cyber-Security Collaborative Research Alliance (Cyber CRA) – ARL
    - Science for Cybersecurity (S4C) – ARL and ARO
    - Science of Security MURI; Trust and Suspicion Basic Research Initiative – AFOSR
  - **Cross-cutting foundations**:
    - Cryptography – DARPA, NIST, NSA, NSF, and ONR
    - Models, standards, testing, and metrics – ARL, ARO, DHS, DOE/OE, NIST, NSF, and OSD

- Foundations of Trust – AFRL, ARL, ARO, CERDEC, DARPA, DOE/OE, NIST, NSA, NSF, ONR, and OSD
- Security Management and Assurance Standards – NIST
- Quantum information science and technology – AFRL, DOE/OE, IARPA, NIST, and ONR
- Cybersecurity education – DHS, NIST, and NSF

- **Maximizing Research Impact**
  - **Supporting national priorities**: The cybersecurity research themes provide a framework for addressing the cybersecurity R&D requirements associated with national priorities in, for example, the healthcare, energy, financial services, and defense sectors.
    - Cybersecurity Education and Workforce Development – DHS, NIST, and NSF
    - Health IT Security Program; National Strategy for Trusted Identities in Cyberspace (NSTIC); Privacy Engineering Initiative; Standards Framework for Critical Infrastructure Protection (Executive Order 13636, "Improving Critical Infrastructure Cybersecurity") – NIST
    - Journal of Sensitive Cybersecurity Research and Engineering (JSCoRE) – ODNI
    - National Critical Infrastructure Security and Resilience R&D Plan (Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience") – DHS and DOE/OE
    - Smart Grid Interoperability Panel - Smart Grid Cybersecurity Committee – DOE/OE and NIST
- **Accelerating Transition to Practice**
  - **Technology discovery, evaluation, transition, adoption, and commercialization**: Explicit, coordinated processes that transition the fruits of research into practice to achieve significant, long-lasting impact.
    - Center for Advanced Communications; National Cybersecurity Center of Excellence (NCCoE) – NIST
    - Cyber Grand Challenge (CGC) – DARPA
    - Cybersecurity for Energy Delivery Systems (CEDS) Program – DOE/OE
    - Cybersecurity research infrastructure - Defense Technology Experimental Research (DETER) testbed, Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), Software Assurance Marketplace (SWAMP); Information Technology Security Entrepreneurs' Forum (ITSEF); Transition to Practice Program – DHS
    - DoD Cyber Transition to Practice Initiative – OSD
    - NSA Technology Transfer Program – NSA
    - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
    - Small Business Innovative Research (SBIR) Conferences – DoD, DHS, and NSF
    - Testbeds and infrastructure for R&D – DARPA, DHS, NSF, and OSD

Planning and Coordination Supporting Request

The CSIA agencies engage in a variety of cooperative efforts – from implementing multiagency testbeds essential for experimentation with new technologies at realistic scales, to collaborative deployment of prototypes, to common standards. The following is a representative summary of current multiagency collaborations:

- **Co-funding**: Defense Technology Experimental Research (DETER) testbed – DHS and NSF; National Centers of Academic Excellence in Information Assurance Education and Research – DHS and NSA

- **Collaborative research**: Cyber-Security Collaborative Research Alliance (CRA) – ARL; Cyber Forensics Working Group – DHS law enforcement components, DoD, FBI, and NIST; NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy – NSF and Intel Corp.; Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) – NSF and Semiconductor Research Corporation; SEI Cyber Research – OSD and Software Engineering Institute
- **Workshops**: Cyber-Physical Systems Public Working Group Workshops – NIST; Cryptographic Key Management Workshop – NIST; Software and Supply Chain Assurance Forum – NIST; Cybersecurity Applications and Technology Conference for Homeland Security – DHS; Small Business Innovation Research (SBIR) Conference – DHS, NIST, and OSD; Annual IT Security Automation Conference – DHS, NIST, and NSA; National Initiative for Cybersecurity Education Annual Workshop – DHS, NIST, NSA, NSF, and OSD; Cloud Forums – DHS, GSA, and NIST; Mobile Security Forum – NIST and NSA; IT Security Entrepreneur Forum, Innovation Summit, SINET Showcase, Transition To Practice Showcase – DHS; Workshops on Incorporating Security Concepts in Undergraduate Computer Science Curriculum – NSF; International Conference on Software Security and Reliability – NIST; Computational Cybersecurity in Compromised Environments (C3E) Workshops – ODNI
- **Collaborative deployment**: Cyber-Physical Systems Global City Teams Challenge / SmartAmerica – NIST; DNS security (DNSSEC) and routing security – AFRL, DHS, and NIST; The National Vulnerability Database – DHS and NIST; U.S. Government Configuration Baseline (USGCB) – NIST and NSA
- **Technical standards**: Developing, maintaining, and coordinating validation programs for cryptographic standards – NIST and NSA; participation in Internet Engineering Task Force security groups to develop standard representations reference implementations of security-relevant data – DHS, NIST, NSA, and OSD; Smart Grid Interoperability Panel - Smart Grid Cybersecurity Committee – DOE/OE and NIST
- **Testbeds**: Continued joint development of research testbeds, such as DETER, Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), Distributed Environment for Critical Infrastructure Decision-making Exercises (DECIDE), Wisconsin Advanced Internet Laboratory (WAIL), Mobile Networks Testbed Emulation – ARL, ARO, CERDEC, DHS, DOE/OE, NSF, ONR, and Treasury
- **DoD Cyber Community of Interest (COI)**: Oversight and coordination of all defensive cyber S&T programs – OSD and DoD Service research organizations
- **Technical Cooperation Program Communications, Command, Control and Intelligence (C3I) Group**: Information assurance and defensive information warfare – AFRL, ARL, ARO, CERDEC, NSA, ONR, and OSD
- **International collaboration**: NSF and the U.S.-Israel Binational Science Foundation joint program; U.S. Army-United Kingdom Network and Information Sciences International Technology Alliance; DHS International Engagements and co-funding activities with Australia, Canada, Germany, Israel, Netherlands, Sweden, United Kingdom, European Union, and Japan
- **Cyber education**: Centers of Academic Excellence – NSA; CyberCorps: Scholarship for Service – NSF; National Initiative for Cybersecurity Education (NICE) – DHS, NIST, NSA, NSF, ODNI, and OSD; Cybersecurity Competitions – DHS; Cybersecurity Organizational/Operational Learning (COOL) – DHS

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the CSIA PCA:

- **AFRL**: Secure systems foundations; foundations for trusted architectures; cyber agility (configuration-based moving target defense, polymorphic enclaves, IP hopping, cyber deception); mission-centric cyber assurance (mission assurance in the cloud, data hiding and analysis, threat abatement, assured resources); Assured by

Design (self-regenerative architecture, science of mission assurance, domain modification, engineering assured systems); mission awareness for mission assurance

- **ARL, ARO, and CERDEC**: Communication and electronic warfare hardware/software convergence security; tactical cyber situational awareness; tactical distributed cloud architecture; software-defined radio protection; software/hardware assurance; cyber cognition; stealthy networked communications; dynamic continuous risk monitoring and risk scoring; trusted social computing; cyber situational awareness; tactical lightweight crypto solutions; tactical PKI enablement; trust research (trust management for optimal network performance); intrusion detection (automated signature generation and anomaly detection)
- **DARPA**: Information Assurance and Survivability (core computing and networking technologies to protect DoD's information infrastructure, and mission-critical information systems; tools and methods to uncover hidden malicious functionality; algorithms for detecting anomalous and threat-related behaviors; more effective user identification and authentication techniques; methods to enable assured and trustworthy Internet communications and computation; and cost-effective security and survivability solutions)
- **DHS**: Cyber transition and outreach (Transition to Practice [TTP]); network and system security integration (security for cloud-based systems, mobile device security, cybersecurity for law enforcement, data privacy and identity management, software quality assurance, usable security and security metrics); trustworthy cyberinfrastructure (Internet measurement and attack modeling, process control system security, secure protocols, distributed denial of service defense); cybersecurity user protection and education (cybersecurity competitions, cybersecurity forensics, data privacy technologies, identity management)
- **DOE/OE**: Continue to align research activities with the DOE-facilitated, energy sector-led *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, updated in 2011, strategic framework and vision that, by 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber-incident while sustaining critical functions
- **IARPA**: Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP); SPAR Program (parsimonious information sharing: minimizing collateral information that must be shared in order to efficiently share a desired piece of information); quantum computer science; trusted integrated circuits
- **NIST**: Foundations (risk management, identity management, key management, security automation, vulnerability management, cryptography); security overlays (healthcare, Smart Grid, cyber-physical systems, public safety networks, trusted identities); security and mobility; continuous monitoring; biometrics; Security Content Automation Protocol; security for cloud computing; security for electronic voting; usable security; supply chain risk management; Big Data Initiative; participation in standards development organizations; techniques for measuring security; metrology infrastructure for modeling and simulation
- **NSA**: Trusted computing (high assurance security architectures enabled by virtualization, improved enterprise protection through strong software measurement and reporting); secure mobility; systems behavior
- **NSF**: Secure and Trustworthy Cyberspace (SaTC) program: a joint program by the NSF Directorates of Computer and Information Science and Engineering (CISE), Mathematical and Physical Sciences (MPS), Social, Behavioral and Economic Sciences (SBE), Education and Human Resources (EHR), and Engineering (ENG) covering all aspects of cybersecurity research and education
- **ONR**: Moving Target decoys and disinformation; non-equilibrium dynamic cyber-interaction; cybersecurity and real-time system theory; machine-assisted situational awareness and planning; real-time virtual machines and real-time cloud provisioning; cyber information infrastructure (resilient autonomic computing, dynamically reconfigurable computing systems, data science, data security, software science, tactical cloud, SOA and beyond, quantum computing, bio / analog computing); proactive cyber-physical system defense

- **OSD**: Cyber Applied Research Program (developing new security methods to integrate Service Laboratory and NSA research for new joint capabilities); assuring effective missions (cyber mission control, effects at scale); cyber agility (autonomic cyber agility, cyber maneuver); cyber resilience (resilient architectures, resilient algorithms and protocols); foundations of trust (system-level trust, trustworthy components and mechanisms); modeling, simulation, and experimentation; embedded, mobile, and tactical; cybersecurity metrics; DoD Cyber Transition to Practice Initiative; and SBIR program and workshop to foster innovation and facilitate networking with small businesses

High Confidence Software and Systems (HCSS)

NITRD Agencies: DARPA, DHS, DoD Service Research Organizations, NASA, NIH, NIST, NSA, NSF, and OSD
Other Participants: DOT, FAA, FDA, FHWA, NRC, and USDA

HCSS R&D supports development of scientific foundations and innovative and enabling software and hardware technologies for the engineering, verification and validation, assurance, standardization, and certification of complex, networked, distributed computing systems and cyber-physical (IT-enabled) systems (CPS). The goal is to enable seamless, fully synergistic integration of computational intelligence, communication, control, sensing, actuation, and adaptation with physical devices and information processes to routinely realize high-confidence, optimally performing systems that are essential for effectively operating life-, safety-, security-, and mission-critical applications. These systems must be capable of interacting correctly, safely, and securely with humans and the physical world in changing environments and unforeseen conditions. In many cases, they must be certifiably dependable. The vision is to realize dependable systems that are precise and highly efficient; respond quickly; work in dangerous or inaccessible environments; provide large-scale, distributed coordination; augment human capabilities; and enhance societal quality of life. New science and technology are needed to build these systems with computing, communication, information, and control pervasively embedded at all levels, thus enabling entirely new generations of engineering designs that can enhance U.S. competitiveness across economic and industrial sectors.

President's FY 2016 Request

Strategic Priorities Underlying This Request

In recent years, the HCSS agencies have engaged in a sustained effort to foster a new multidisciplinary research agenda that will enable the United States to lead in the development of next-generation engineered systems that depend on ubiquitous cyber control and require very high levels of system assurance. Through a variety of ongoing activities, the HCSS effort is forging a nationwide community interested in the CPS research challenges faced in common across such economic sectors as medicine and healthcare, energy, transportation, manufacturing, and agriculture, and across such agency missions as national security, environmental protection, and space exploration. The HCSS agencies have set the following priorities for research coordination:

- **Science and technology for building cyber-physical systems**: Develop a new systems science providing unified foundations, models and tools, system capabilities, and architectures that enable innovation in highly dependable cyber-enabled engineered and natural systems; develop public domain, cyber-physical testbeds
- **Management of complex and autonomous systems**: Develop measurement and understanding for improved models of complex systems of systems, shared control and authority, levels of autonomy, human-system interactions, and integrated analytical and decision-support tools; integrate computer and information-centric physical and engineered systems
- **Assurance technology**: Develop a sound scientific and technological basis, including formal methods and computational frameworks, for assured design, construction, analysis, evaluation, and implementation of reliable, robust, safe, secure, stable, and certifiably dependable systems regardless of size, scale, complexity, and heterogeneity; develop software and system-engineering tool capabilities to achieve application and problem domain-based assurance, and broadly embed these capabilities within the system engineering process; reduce the effort, time, and cost of assurance ("affordable" verification and validation [V&V]/certification); provide a technology base of advanced-prototype implementations of high-confidence technologies to spur adoption; design and install resilient energy delivery systems capable of surviving a cyber-incident while sustaining critical functions; support development of regulations and guidance for assurance of safety and security

- **High-confidence real-time software and systems**: Pursue innovative design, development, and engineering approaches to ensure the dependability, safety, security, performance, and evolution of software-intensive, dynamic, networked control systems in life- and safety-critical infrastructure domains, including systems-of-systems environments; real-time embedded applications and systems software; component-based accelerated design and verifiable system integration; predictable, fault-tolerant, distributed software and systems; modeling of heterogeneous distributed systems using unified mathematical framework; develop safety assurance tools and techniques to build justifiable confidence in aerospace and national airspace systems; develop infrastructure for medical device integration and interoperability, patient modeling and simulation, and adaptive patient-specific algorithms
- **Translation into mission-oriented research**: Leverage multiagency research to move theory into practice, using challenges and competitions, for example, to solve problems in domains such as energy, cyber-physical ground and air transportation systems, and connected vehicle-to-infrastructure systems
- **CPS education**: Launch an initiative to integrate CPS theory and methodology into education and promote increased understanding of and interest in CPS through the development of new curricula at all levels that engage both the physical and cyber disciplines and foster a new generation of U.S. experts

Highlights of the Request

The HCSS agencies report the following topical areas as highlights of their planned R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **Cyber-physical systems**: Explore the fundamental scientific, engineering, and technological principles that underpin the integration of cyber and physical elements, making the "systems you can bet your life on" possible; continue support for research to enable physical, biological, and engineered systems whose operations are integrated, monitored, and/or controlled by a computational core and interact with the physical world, with components networked at every scale and computing deeply embedded in every physical component, possibly even in materials; real-time embedded, distributed systems and software; CEMMSS to model and simulate systems interdependent with the physical world and social systems; safety models and designs for cyber-physical medical systems, including interoperable ("plug-and-play") medical devices – DARPA, DoD Service research organizations, FDA, NASA, NIH, NIST, NSA, NSF, OSD, and VA
- **Complex systems**: Multiyear effort, including focus on software for tomorrow's complex systems such as CPS, to address challenges of interacting systems of systems, including human-system interactions, and investigate their non-linear interactions and aggregate or emergent phenomena to better predict system capabilities and decision-making about complex systems; develop new algorithms for functional analysis of real-time software, control effects of multicore memory access on CPS real-time behavior, and flexible and predictable control of multiple, semi-autonomous UAVs; joint capability technology demonstration of flexible mission-reprogramming, increased endurance, and increased autonomy – AFRL, FAA, NASA, NIH, NIST, NSF, and OSD
- **High-confidence systems and foundations of assured computing**: Formal methods and tools for modeling, designing, measuring, analyzing, evaluating, and predicting performance, correctness, efficiency, dependability, scalability, safety, security, and usability of complex, real-time, distributed, and mobile software and systems; high-assurance environments from COTs; high-assurance virtualization and measurement; architectures, components, composition, and configuration; engineering, analysis, and testing of software and hardware; architecture, tools, and competence for assurance certifiable safe systems; cost-effective V&V; verification techniques for separation assurance algorithms; safety cases, standards, and metrics; quantum information processing – AFOSR, AFRL, ARO, DARPA, FDA, NASA, NIH, NIST, NSA, NSF, ONR, and OSD

- **Information assurance requirements**: Methods and tools for constructing, analyzing security structures (management architectures and protocols, etc.); assurance technologies for cross-domain creation, editing, sharing of sensitive information in collaboration environments that span multiple security levels; cryptographic algorithms and engineering; assured compilation of cryptographic designs, specifications to platforms of interest - NSA and ONR; testing infrastructure for health IT standards, specifications, certification (with HHS); cross-enterprise document sharing in electronic health systems; standards and quality measurement systems for smart manufacturing, measurement science and standards for CPS engineering; build a testbed to help industry, university, and government collaborators develop an open standards platform to facilitate the simultaneous engineering of the physical and virtual components of manufacturing systems – NIH, NIST, and NSF
- **Aviation safety**: R&D in transformative V&V methods to rigorously assure the safety of aviation systems. This includes considerations for all classes of aircraft and anticipated future air traffic management capabilities; and develop and demonstrate innovative technologies in the design of architectures with advanced features, focusing on designing for high-confidence, standardization, and certification – AFRL, FAA, NASA, and OSD
- **Assurance of Flight-Critical Systems (AFCS)**: Provide appropriate airworthiness requirements for Unmanned Aircraft Systems (UAS) that help enable routine access to the National Airspace System (NAS); enable assurance that new technologies envisioned for the Next Generation Air Transportation System (NextGen) are as safe as, or safer than, the current system and provide a cost-effective basis for assurance and certification of complex civil aviation systems; develop and analyze formal models of air traffic management systems for safety properties incorporating the effects of uncertainty – AFRL, FAA, and NASA

Planning and Coordination Supporting Request

To build multidisciplinary communities of interest both within and across sectors, the HCSS agencies have developed a busy annual schedule, which will continue through FY 2016, of workshops and other research meetings that bring a broad mix of stakeholders together. The HCSS workshops on high-confidence medical devices, for example, draws medical researchers, medical practitioners and caregivers, device developers and vendors, care facility administrators, academic computer scientists and engineers, and Federal Government regulators. These unique gatherings are forging wider understanding of critical issues and developing consensus around promising research directions in high-confidence CPS. Similarly, HCSS-sponsored workshops on transportation CPS are developing agreement on R&D needs that span multiple transportation sectors. In summary, the following are ongoing HCSS coordination activities:

- **National Research Workshop Series**: Academic, industry, and government stakeholder workshops to identify new R&D for building 21st century CPS for life-, safety-, and mission-critical applications; topics include:
  - **High Confidence Medical Device CPS** – National Workshop on Research Frontiers in Medical Cyber-Physical Systems – FDA, NIST, NSA, and NSF
  - **Future Energy CPS** – National Workshop on Energy Cyber-Physical Systems – NIST, NSA, and NSF
  - **High Confidence Transportation CPS**: National Workshop on Transportation Cyber-Physical Systems – AFRL, DOT, FAA, FDA, FHWA, NASA, NIST, NSA, and NSF
  - **CPS Week** – Annual High Confidence Networked Systems (HiCoNS) meeting – AFRL, DHS, NASA, NIST, NSA, and NSF
  - **Static Analysis Tools Exposition (SATE)**: Annual summit on software security for vendors, users, and academics – NIST, NSA, and NSF in collaboration with DHS
  - **CPS Education**: NSA, NSF, and ONR

- **Scholar In Residence Program** – FDA and NSF
- **Software Assurance Metrics and Tool Evaluation**: Annual workshop for users and developers to compare efficacy of techniques and tools; develop vulnerability taxonomies – DHS, NIST, and NSA
- **Safe and Secure Software and Systems Symposium (S5)**: Industry, academia, and government collaborate on improving the airworthiness and assurance certification process of future aerospace flight control systems with both incremental and revolutionary technological innovations in safety and security V&V techniques that support maintaining cost and risk at acceptable levels – AFRL, NASA, NSA, and NSF
- **Annual HCSS Conference**: Showcasing of promising research to improve system confidence – FAA, NASA, NSA with NSF, ONR, and OSD
- **Software Assurance Forum**: Coordinate software certification initiatives and activities for Systems containing Software (ScS) – DHS, DoD Service research organizations, NIST, NSA, and OSD
- **Safety of flight-critical systems**: Workshops and technical discussion – AFRL, NASA, NSA, and NSF
- **Standards, software assurance metrics for Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS)**: Collaborative development – NIST and others
- **Biomedical imagery**: Technical standards for change measurements in patient applications – FDA, NIH, and NIST
- **Cooperative proposal evaluation** – AFRL, DARPA, FAA, FDA, NASA, NIST, NRC, NSA, NSF, and OSD
- **FAA National Software and Airborne Electronic Hardware Standardization Conference** – FAA, NASA, and OSD
- **NASA Formal Methods Symposium (NFM 2015)** – AFRL, FAA, FDA, NASA, NIST, NSF, NSA, and OSD
- **Exploratory Advanced Research (EAR) Program**: Connected Highway Vehicle System concepts, with human and hardware-in-the-loop, and adaptive hardware, structures, and pavements – DOT, FHWA, NIST, and NSF
- **National Robotics Initiative (NRI)**: Cross-cutting program to accelerate the development and use of robots that work beside, or cooperatively with, people – NASA, NIH, NSF, and USDA

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the HCSS PCA:

- **AFRL**: Develop technologies to support the verification, validation, and ultimately certification of increasingly autonomous, flight-critical systems operating in dynamic, uncertain, cooperative, and contested environments. Develop alternate arguments of assurance from innovative, usable, and more cost effective formalized mathematical frameworks, shifting the assurance burden from traditional test-based verification. Develop methods and tools to construct precise, mathematically rigorous requirements in order to automatically evaluate them for testability, traceability, and de-confliction. Develop technologies that provide formal assurance of appropriate decisions with traceable evidence at every level of design. Develop methods to assure un-verifiable, highly complex, autonomous systems through run time assurances, or run time monitoring, just-in-time prediction, and mitigation of undesired decisions and behaviors
- **DARPA**: Develop technologies to secure mission-critical embedded computing systems in ground vehicles and unmanned aerial vehicles. Use recent advances in program synthesis, formal verification techniques, and low-level and domain-specific programming languages to produce fully verified operating systems for embedded devices

- **FAA**: Improve and maintain methods for approving digital systems for aircraft and air traffic control (ATC) systems and prepare for the Next Generation Air Transportation System (NextGen) by conducting research in advanced digital (software-based and airborne electronic hardware [AEH]-based airborne systems) technology; keep abreast of and adapt to the rapid, frequent changes and increasing complexity in aircraft and ATC systems; understand and assess safe implementations in flight-essential and flight-critical systems (e.g., fly-by-wire flight controls, navigation and communication equipment, autopilots, and other aircraft and engine functions); and continue work on digital requirements for software-development techniques and tools, airborne electronic hardware design techniques and tools, onboard network security and integrity, and system considerations for complex digitally intensive systems
- **FDA**: Formal methods-based design (assured verification, device software and system safety modeling and certification, component composition, forensics analysis, engineering tool foundations); architecture, platform, middleware, resource management for interoperable medical devices (plug-and-play, vigilance and trending systems); infrastructure for medical-device integration, interoperation; patient modeling, simulation; adaptive patient-specific algorithms; and black box/data loggers and analysis
- **FHWA**: Continue to apply concepts from fundamental advances in cyber-physical science to develop a new transportation paradigm of connected highway and vehicle systems in support of broad mission goals, including making traffic deaths or serious injuries rare events, optimizing mobility so that personal travel and goods movement are easy and reliable within, between, and across modal systems, and reducing the energy and resources required for highway transportation in the U.S. Also enhance research, development, and technology for health monitoring of highway transportation structures and pavements to include control from the nano through micro to the macro scale to create true, fully functioning cyber-physical systems that will ensure a state of good repair for the Nation's roads and respond to both every day and extreme environmental changes
- **NASA**: Perform R&D activities to enable high confidence in aviation systems supporting safe, efficient growth in global operations; real-time, system-wide safety assurance; and assured autonomy for aviation transformation. Specific activities include: maturation of assurance case techniques for use on complex aviation systems; advancing formal methods techniques for assuring complex software-intensive systems; advancing assurance technologies to enable deployment of UAS in the NAS; and design and analysis of operational procedures, algorithms and enabling technologies for air traffic control
- **NIH**: Translational research in biomedical technology to enhance development, testing, and implementation of diagnostics and therapeutics that require advanced CPS innovations; assurance in medical devices such as pulse oximeters and infusion pumps, cardio-exploratory monitors for neonates; telemedicine; computer-aided detection and diagnosis; computer-aided surgery and treatment; neural interface technologies such as cochlear implants, and brain-computer interfaces. Systematic exploration of the sources and variability introduced during tumor image acquisition and tumor size measurement, for the development of improved algorithms used in assessment of new therapies; and development of new data acquisition and analysis methods to aid in the determination of optimal ultrasound exposure settings to obtain the necessary diagnostic information by using the very lowest total energy for increased patient safety
- **NIST**: Cyber-Physical Systems Public Working Group, Global City Teams Challenge, and a CPS testbed to advance measurement science and standards enabling CPS development and deployment; Cybersecurity for Smart Manufacturing Systems to help secure industrial control systems used in manufacturing and CPS; Software Assurance Metrics and Tool Evaluation (SAMATE – with DHS funding) and Software Assurance Reference Dataset (SARD) to help provide confidence that software is free from vulnerabilities; National Vulnerability Database; Internet infrastructure protection (with DHS funding); seamless mobility; trustworthy information systems; information security automation, Security Content Automation Protocol (SCAP); combinatorial testing; next-generation access control; smart manufacturing

- **NRC**: Regulatory research to aid safety and security in cyber-physical systems (digital instrumentation and control systems) used in the nuclear energy sector
- **NSA**: High-assurance system design (correct-by-construction methods, model-driven development, programming languages) and analysis (concolic execution, multi-tool analysis, separation/matching logic, static/dynamic analysis), with focus on usability; assured implementation, execution of critical platform components and functionality; and assured cryptographic implementations (software and hardware); domain-specific workbench developments (cryptography, guards, protocols)
- **NSF**: Joint research program of CISE and ENG directorates addressing CPS challenges in three areas (foundations; methods and tools; and components, run-time substrates, and systems); form partnerships to support advanced manufacturing through CPS research that helps better integrate IT into manufactured goods; core research in software and information foundations, communications, and computer systems; Expeditions projects in next-generation approaches to software and system assurance and CPS; Secure and Trustworthy Computing (SaTC) to ensure security, reliability, privacy, and usability; create core disciplinary, exploratory, and educational programs; and the National Robotics Initiative (NRI) to accelerate the development and use of robotics cooperatively with people
- **OSD**: Improve the DoD's ability to design, build, test, and sustain software-intensive cyber-physical systems that meet DoD mission-critical requirements for embedded and distributed systems, exhibit predictable behavior, and enable affordable evolution and interoperability; includes specification of complex requirements; "correct-by-construction" software development; scalable composition; high-confidence software and middleware; system architectures for network-centric environments; technologies for system visualization, testing, verification, and validation; model- and platform-based design and development approaches; and tools for controlling automated exploration and evaluation of massive trade spaces

High End Computing Infrastructure and Applications (HEC I&A)

NITRD Agencies: DoD (HPCMP), DoD Service Research Organizations, DOE/NNSA, DOE/SC, EPA, NASA, NIH, NIST, NOAA, NSF, and OSD

HEC I&A agencies coordinate Federal activities to provide advanced supercomputing systems, applications software, extreme-scale data management and analysis, and HEC R&D infrastructure to meet Federal agency mission needs and support national competitiveness. HEC infrastructure enables researchers in academia, industry, Federally Funded Research and Development Centers (FFRDCs), and Federal institutions to model and simulate complex processes and analyze extreme scale data over a broad spectrum of disciplines in national security, science, engineering, and industrial design and development. Advances in HEC technologies impact the entire spectrum of computing devices, from the largest systems to hand-held devices, allowing the most powerful computing platforms to become more affordable and smaller devices more powerful over time. The Federal HEC infrastructure also serves as critical infrastructure supporting diverse initiatives associated with national priorities such as cybersecurity, understanding the human brain, big data, climate science, nanotechnology, the Materials Genome Initiative, and advanced manufacturing.

President's FY 2016 Request

Strategic Priorities Underlying this Request

Investments in Federal HEC facilities, advanced applications, and next-generation computing technologies and systems support national competitiveness and provide the means for industry, academia, and Federal laboratories to apply advanced computational capabilities in support of Federal agencies' diverse science, engineering, and national security missions. They also provide the government with the flexibility and expertise to meet new challenges as they emerge. Priorities include:

- **Leadership-class and production HEC systems**: Provide HEC systems with capabilities and capacities needed to meet critical agency mission needs and support the national science and engineering research communities, U.S. industry, and academic research; ensure that emerging computer technologies support industrial, national security, and scientific applications and reduce energy requirements for and climate impact of computing technology at all scales. U.S. leadership in HEC systems is critical for maintaining U.S. competitiveness as a growing number of nations around the world increase their investments to develop and deploy indigenous HEC systems and applications, threatening U.S. computing industries
- **Advancement of HEC applications**: Support the computational requirements of disciplines including national security, financial modeling, aerospace, astronomy, biology, biomedical science, chemistry, climate and weather, ecological computation, geodynamics, energy and environmental sciences, materials science, measurement science, nanoscale science and technology, physics, and other areas to make breakthrough scientific and technological discoveries and address national priorities. Develop scientific and engineering algorithms and applications software and tools for current and next-generation HEC platforms; develop mission-responsive computational environments; and lead critical applied research in algorithms and software for emerging architectures in order to preserve the performance of existing codes
- **Leading-edge cyberinfrastructure**: Provide efficient, effective, and dependable access to HEC facilities and resources for user communities across a wide variety of skills and backgrounds in industry, academia, and Federal institutions; develop capabilities and enhance infrastructure for computational and data-enabled science, modeling, simulation, and analysis; and share best practices for managing and enhancing HEC resources in a cost-effective and energy-efficient manner

- **Broadening impact**: Conduct crosscutting activities by the HEC I&A agencies, individually or collectively, that span multiple major priorities and serve to extend the breadth and impact of high end computing to meet the Nation's highest science, engineering, national security, and competitiveness priorities

Highlights of the Request

The HEC I&A agencies report the following areas as highlights of their planned investments for FY 2016 under each of the main HEC I&A priorities. Agencies are listed in alphabetical order:

- **Leadership-class and production HEC systems**
  - **DoD (HPCMP)**: Provide modern, large-scale, stable computational resources in DoD supercomputing centers nationwide. Procure multiple, multi-petaflop (PF), large-scale enterprise high performance computing (HPC) systems for DoD's Research, Development, Test, and Evaluation (RDT&E) community. Provide application support, data analysis and visualization, and HPC system expertise at five DoD Supercomputing Resource Centers
  - **DOE/NNSA**: Provide mission-responsive computational environment for NNSA stockpile stewardship program. Deploy LANL/SNL Trinity Advanced Technology System (44 PF); accept hardware delivery of LLNL Sierra Advanced Technology System (150 PF); deploy Commodity Technology System scalable units (for capacity computing) across NNSA tri-labs
  - **DOE/SC**: Acquire and operate increasingly capable computing systems, starting with multi-petaflop machines that incorporate emerging technologies from research investments. Site preparation activities will continue for 75 PF - 200 PF upgrades at each Leadership Computing Facility; NERSC will take delivery of the NERSC-8 supercomputer, which will expand the capacity of the facility by 10 PF - 40 PF to address emerging scientific needs
  - **NASA**: Provide HEC resource and service support across the entire spectrum of users and their diverse requirements. Install hardware that provides world-class performance in capability, capacity, and time-critical computing
  - **NIH**: Continued support for broad-based HEC I&A for biomedical computing applications. Continuation and growth of the NIH Big Data to Knowledge (BD2K) program. Extension and modernization of NIH campus high end computing facilities and networking, predominantly to serve the intramural community
  - **NOAA**: Provide computational systems to support improved predictive services for weather, climate, hurricane, and ecosystem environmental forecasts. Continue to operate Gaea 1400 Teraflops (TF) Climate Computing HPC (at DOE's Oak Ridge National Laboratory [DOE/ORNL]); Jet 340 TF Hurricane Forecast Improvement Project (HFIP); allocation on DOE/SC's Titan HPC (roughly equivalent to 500 TF); transition models to Theia 1000 TF Sandy Supplemental HPC; expand Theia with another 1000 TF of fine-grained computing; retire Zeus (383 TF Weather and Climate HPC)
  - **NSF**: Provide world-class computational resources to enable major scientific advances. Major continuing resources include leadership-class Blue Waters at University of Illinois; Stampede at Texas Advanced Computing Center (TACC), and a diverse set of additional resources for computation, data, and visualization; eXtreme Science and Engineering Discovery Environment (XSEDE), Technology Audit Service (TAS) for productivity enhancement and community building; other resources include Yellowstone at National Center for Atmospheric Research (NCAR) and Open Science Grid (OSG). Recent computational and data resources include Comet, a 2 PF compute resource at SDSC, and Wrangler, a 10 PB data resource at TACC; new HEC system acquisitions, including Bridges at Pittsburgh Supercomputing Center and Jetstream at Indiana University

- **Advancement of HEC applications**
  - **DoD (HPCMP)**: Mature and demonstrate large and smaller scale software development and system management applications. Multi-physics applications development for acquisition engineering community in air vehicles, ground vehicles, ships, and RF antennas; smaller scale application software development projects to enable the DoD RDT&E community to effectively use next-generation hardware; programming environments, system software, and computational skills transfer for both DoD workforce development and S&T application modernization; Frontier Projects combining multi-billion hour allocations with technology transfer and development to advance state-of-the-practice in the application of HPC to the DoD's most challenging problems
  - **DOE/NNSA**: Co-design for and analysis of application performance impacts by advanced architectures, via proxy apps, programming models, resilience techniques, burst buffers, etc.
  - **DOE/SC**: Prepare today's scientific and data-intensive computing applications for exascale system through partnership (SciDAC) investment in exascale co-design centers. Conduct research, development, and design efforts in applied mathematics with focus on new mathematics required to more accurately model systems and algorithm innovations that increase energy efficiency and resilience of future-generation supercomputers and support analysis of extreme scale data
  - **EPA**: Mission-related scientific applications including analytics and computer science required for extreme-scale mission-related research programs in air quality, emissions, climate research, and interactions with human health; advanced distributed, massive volume data and modeling capabilities with initial applications to support Air Program goals
  - **NASA**: Optimize science and engineering workflows on high-end computing, including assistance to migrate codes to many-core architectures; invest in system and application performance tools that enable full understanding of system and application performance; provide data analysis and visualization tools and support that enable exploration of huge data sets
  - **NIH**: Scientific computing efforts such as biomolecular modeling, physiological modeling, and multiscale modeling that use HEC resources or are in pre-HEC state
  - **NIST**: Measurement science to speed development and industrial applications of advanced materials; Materials Genome Initiative (development of modeling and simulation techniques, tools; verification and validation, uncertainty quantification [VVUQ]); Advanced Materials Center of Excellence (modeling and informatics to accelerate materials discovery and deployment); measurement infrastructure for HEC software (VVUQ); measurement science for visualization (hardware - uncertainty quantification, calibration, and correction; software - uncertainty quantification and visual representation, quantitative methods in visualization)
  - **NOAA**: Improve model-based computing of weather and hurricane forecasting and climate prediction
  - **NSF**: Advance HEC applications broadly, including in areas of national priority, such as the BRAIN (Brain Research through Advancing Innovative Neurotechnologies) Initiative, food and water, and energy security. Supporting programs include: CIF21 – meta-program to coordinate the full cyber-ecosystem across NSF; CDS&E - Computational and Data-Enabled Science and Engineering meta-program across many NSF units; SI^2 – developing and using sustainable software, with a new focus on Software Institutes, the largest of three categories of awards
  - **OSD**: Advancements in modeling and simulation of challenging environments, algorithm and technology development, and big data applications

- **Leading-edge cyberinfrastructure**
  - **DoD (HPCMP)**: Maintain world-class wide-area R&D network to provide access to DoD supercomputing centers - Defense Research and Engineering Network (DREN) at 100 Gbps; cybersecurity operations; frameworks for productivity of non-expert users to enable broader application of HEC-enabled solutions
  - **DOE/NNSA**: Maintain common computing environment across NNSA labs
  - **EPA**: Infrastructure to combine existing and future data with various temporal and spatial scales, develop and run regional to global models across computational platforms at all scales
  - **NIH**: Continue investment in scientific computing, e.g., software development, neuroscience solicitations, grid computing; National Cancer Institute (NCI) Cancer Genomics Cloud Pilots
  - **NOAA**: Continue to leverage nationwide high-bandwidth, low-latency network to promote cross-agency, shared use of HPC
  - **NSF**: CIF21 provides a comprehensive, integrated, sustainable, and secure cyberinfrastructure to accelerate research and education and new functional capabilities in computational and data-intensive science and engineering; XSEDE – eXtreme Science and Engineering Discovery Environment; CDS&E – Computational and Data-Enabled Science and Engineering meta-program across many NSF units; SI^2 – creating a software ecosystem spanning from embedded sensors to HEC to major instruments and facilities
- **Broadening impact**
  - **DoD (HPCMP)**: Develop next-generation computational workforce within DoD via skills development, deployment of both computational and domain-specific expertise to the DoD RDT&E complex, and investments in tools and expertise that match HPC environments to user workflow
  - **DOE/SC**: Collaborate with other Federal agencies to ensure broad applicability of capable exascale computing across the U.S. Government; develop next-generation computational science workforce through support of the Computational Science Graduate Fellowship in partnership with DOE/NNSA
  - **NASA**: Coordinate with other HEC agencies on initiatives to maintain and enhance U.S. HEC leadership
  - **HEC agencies**: Continue to advance research and technology in VVUQ; improve user training
  - **NSF**: Education, training, and outreach activities, led by awards such as XSEDE, supporting the current and next generation workforce

Planning and Coordination Supporting Request

Since 2005, the HEC agencies have provided tens of billions of computing hours on the Nation's most powerful computing platforms to enable researchers from academia and industry to address ultra-complex scientific challenges; coordinating this activity remains a major focus of collaboration among the HEC agencies and these stakeholders. Another key focus is selecting, evaluating, procuring, and operating Federal high-end platforms – a complicated, labor-intensive process that the HEC agencies work closely together to streamline. A third major focus of collaborative activities is development of sharable computational approaches for investigation and analysis across the sciences. Cooperative activities under each of the HEC I&A strategic priorities include:

- **Leadership-class and production HEC systems**
  - **Leadership-class and production computing**: Coordination to make highest capability HEC resources available to the broad research community and industry – DoD (HPCMP), DOE/NNSA, DOE/SC, NASA, NIST, NOAA, and NSF

- **System reviews, benchmarking, metrics**: Collaborations – DoD (HPCMP), DOE/NNSA, DOE/SC, NASA, NOAA, NSA, and NSF
- **DOE interagency collaboration**: Multi-agency review of the DOE/NNSA and DOE/SC preliminary plan for the Exascale Computing Initiative (ECI) – DoD (HPCMP), NASA, NIH, NOAA, NSA, and NSF
- **DOE intra-agency collaborations**: Joint system procurements for next advanced technology systems delivered in 2017 and co-design for future systems – DOE/NNSA and DOE/SC

- **Advancement of HEC applications**
  - **DOE intra-agency collaborations**: SciDAC-3 institutes and partnerships continue – DOE/NNSA and DOE/SC
  - **DOE/SC computing facilities**: Provide over 11 billion core hours in 2015. NERSC – 2.575 billion core hours; OLCF – 3.350 billion core hours; ALCF – 5.150 billion core hours
  - **Multiscale modeling in biomedical, biological, and behavioral systems**: Interagency collaboration to advance modeling of complex living systems – DoD, NIH, and NSF
  - **INCITE**: Allocate hours for projects such as climate, weather, and water model runs – DOE/SC and NOAA, and study of flow of suspensions – DOE/SC and NIST
  - **XSEDE, Petascale Computing Resource Allocations (PRAC)**: Provide 4-5 billion core compute hours to the open science community, spanning research of multiple agencies; all disciplines represented – HEC agencies and other agencies
  - **Computational toxicology**: Integration of HEC technologies with molecular biology to improve methods for risk assessment of chemicals – DoD, DOE/SC, FDA, and NIH
  - **Earth System Modeling Framework (ESMF) and Earth Systems Grid Federation (ESGF)**: DoD, DOE/SC, NASA, NOAA, and NSF
  - **Simulation study of cement hydration**: NIST and NSF
- **Leading-edge cyberinfrastructure**
  - **Remote Sensing Information Gateway (RSIG)**: Allows users to integrate their selected environmental datasets into a unified visualization – DOE/SC, EPA, NASA, and NOAA
- **Broadening impact**
  - **Interagency participation in proposal review panels, principal investigator meetings** – HEC agencies
  - **Extending awareness**: Explore ways to increase awareness of the importance of U.S. HEC leadership – HEC IWG
  - **Explore ways to maximize HEC resources for compute and data allocations** – HEC IWG
  - **Strategic planning**: Participate in strategic initiatives to maintain U.S. HEC leadership – HEC agencies
  - **Education/workforce development**: Support a Federal HEC inventory/portal for learning and workforce development resources – HEC IWG
  - **Metrics**: Explore alternatives to Linpack benchmark to establish more meaningful measures for performance of U.S. HEC systems – HEC IWG
  - **Green computing**: Promote energy-efficient "green" computing practices and explore methods to dramatically reduce HEC energy consumption and related energy costs – DoD (HPCMP), DOE/SC, and NASA

- **Technology transfer**: Transfer of computational skills and technologies to partners in industry and academia – HEC agencies

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the HEC I&A PCA:

- **DoD (HPCMP)**: HEC services for RDT&E community (e.g., platforms, computational science software support); computational science institute for DoD priorities (blast protection)
- **DOE/NNSA**: Operate the ASC Cielo system (1.4 PF) at LANL and Sequoia system (20 PF) at LLNL
- **DOE/SC**: Operate Hopper (1.3 PF) and Edison (2.4 PF) systems at LBNL, the Mira (10 PF) system at ANL, and the Titan (27 PF) system at ORNL
- **EPA**: HEC modeling in environmental restoration, sustainability, exposure in human and ecological systems, and others (atmosphere, land, fresh water); tools for algorithm development and deployment and databases and techniques for use with HEC
- **NASA**: Augment Pleiades supercomputer at NAS (NASA Ames) in FY 2015 (to over 5 PF peak); explore hybrid cloud-computing capability in HEC environment, focusing on big data applications
- **NIH**: Fund predominantly broad-based biocomputing awards; implement recommendations for the NIH Big Data to Knowledge (BD2K) Initiative, as directed
- **NIST**: Parallel and distributed algorithms and tools for measurement science, including fundamental mathematics, uncertainty quantification, image analysis, materials science, and virtual measurement laboratory
- **NOAA**: Investments in applied research projects in the areas of adoption of advanced computing, communications, and information technology
- **NSF**: Provide advanced compute, data, and visualization resources from campus-level to leadership-class; enhance productivity and broaden participation (XSEDE); advance and sustain software and application ecosystem (CDS&E and SI^2); coordinate the full cyber-ecosystem across NSF (CIF21 - Meta-program)
- **OSD**: Incorporate Electromagnetic Spectrum (EMS) object models and target folder utilizing cloud-based data processing; autonomous systems for daily military operations, including force protection and special operations

High End Computing Research and Development (HEC R&D)

NITRD Agencies: DARPA, DoD (HPCMP), DoD Service Research Organizations, DOE/NNSA, DOE/SC, NASA, NIH, NIST, NOAA, NSA, NSF, and OSD
Other Participants: IARPA

HEC R&D agencies conduct and coordinate hardware and software R&D to enable the successful development and effective use of future high-end systems capabilities and drive solutions in support of national security, economic competitiveness, science, engineering, and projected Federal agency mission needs. HEC R&D takes aim at many of society's long-term challenges and contributes to strengthening the Nation's leadership in science, engineering, and technology. Research areas of interest include promising future computational systems such as quantum information science, superconducting supercomputing, and biological computing; programming environments that increase developer productivity and ability to program at scale; system software, applications, and system architectures that effectively utilize up to billion-way concurrency; reducing system energy by orders of magnitude; achieving system resilience at embedded and extreme scales; heterogeneous accelerated and scalable systems for extreme performance; and enabling future revolutions in simulation, data analytics, and big-data-enabled applications and technology.

President's FY 2016 Request

Strategic Priorities Underlying This Request

For decades, HEC R&D agencies have led development of increasingly capable computing technologies, user environments, and applications that have impacted the entire computing industry. These advances not only enhanced mission success but also enabled and motivated increased HEC usage by industry and academia, promoting economic competitiveness, national security, and scientific leadership. Now, the HEC community faces great challenges in creating effective high-end systems using technology that is driven primarily by the consumer marketplace. New high-end systems will require advances in energy efficiency, data movement, concurrency, resilience, security, and programmability. These challenges must be met to achieve and exploit the orders of magnitude increase in HEC capability that are needed to solve increasingly data-intensive and complex problems for science, engineering, manufacturing, and national security. To address the growing complexity and long-term costs of emerging platforms, HEC researchers seek to exploit heterogeneous advanced processor technologies, novel memory and storage technologies, and innovative approaches to software creation, and to innovate to overcome challenges of energy consumption, reliability, and scalability. Given these challenges, the HEC R&D agencies see the following as key research priorities for FY 2016:

- **Extreme-scale computation**: Integrate computer science and applied mathematical foundations to address the challenges of productive and efficient computation from the embedded through the exascale level and beyond. Develop innovative systems that combine increased speed, efficient use of energy, data centric techniques, economic viability, high productivity, and robustness to meet future agency needs for systems that manage and analyze ultra-large volumes of data and run multiscale, multidisciplinary science and engineering simulations and national security applications. Explore new concepts and approaches for solving technical challenges such as power use, efficient data placement and utilization, heterogeneous domain-specific performance acceleration, thermal management, file system I/O bottlenecks, resiliency, highly parallel system architectures with support for up to billion-way concurrency, and programming language and software development environments that can increase the usability and utility of large-scale multiprocessor (including hybrid) systems. Develop, test, and evaluate prototype HEC technologies, systems, and software to reduce industry and end-user risk and to increase technological competitiveness. Implement critical technology R&D partnerships for extreme-scale readiness

- **New directions in HEC hardware, software, computer science, and system architectures**: Develop novel scientific frameworks, power-efficient system architectures, heterogeneous and specialized system acceleration, programming environments, measurement science, thermal management, and hardware and software prototypes to take computing performance and communications "beyond Moore's Law" and to advance potential new breakthroughs in biological, quantum, and superconducting computing
- **Productivity**: Continue collaborative development of new metrics of system performance, including benchmarking, lessons learned for acquisition, and reducing total ownership costs of HEC systems; integrate resources for improved productivity among all users. Design and develop requirements for workflow systems and software to enable, support, and increase the productivity of geographically dispersed collaborative teams that develop future HEC applications
- **Broadening impact**: Conduct crosscutting activities by the HEC R&D agencies, individually or collectively, that span multiple major priorities and serve to extend the breadth and impact of high end computing to meet the Nation's highest science, engineering, national security, and competitiveness priorities, including expanding the HPC workforce

Highlights of the Request

The HEC R&D agencies report the following areas as highlights of their planned research investments for FY 2016 under each of the main HEC R&D priorities. Agencies are listed in alphabetical order:

- **Extreme-scale computation**
  - **DARPA**: DARPA investments aim to prevent technological surprises to the U.S. by pursuing breakthrough technologies. Explore new architectures, power efficient technologies, and systems, enabling thermal efficiency, data centric architectures and techniques, resiliency management, new packaging technologies, new interconnect technologies, and better human interfaces
  - **DoD (HPCMP)**: Collaborative funding of application development environments and algorithms, runtime environments, and system software for extreme-scale computing
  - **DOE/NNSA**: Implement critical technology R&D partnerships for exascale readiness to ensure sustained application performance. Initiating next round of R&D vendor partnerships on next-generation node, memory and system engineering research; advancing state-of-the-art HPC software technologies, such as compilers, file systems, and tools for exascale computing
  - **DOE/SC**: Research & Evaluation Prototypes (REP) program to competitively select R&D partnerships with U.S. computer vendors to initiate the design and development of node and system designs suitable for exascale systems; computer science research to develop capable exascale systems, with focus on data-intensive science challenges; tools for software development and system design; user interfaces; software stacks for development and execution that dynamically deal with time-varying energy efficiency and reliability requirements, including operating systems, file systems, compilers, and performance tools; and visualization and analytics to enable understanding of extreme scale datasets; SciDAC Institutes and partnerships continued
- **New directions in HEC hardware, software, computer science, and system architectures**
  - **DARPA**: Research computing technologies critical to enable data intensive embedded systems including energy efficient technologies and architectures; unconventional computation and data representations based on probabilistic inference; thermal techniques and approaches; photonic-based technologies and architectures; cybersecurity and anti-tamper technologies; data-centric processing; biologically based research developments; high performance processing fabrication alternatives; reliability; domain-

specific processing optimizations including specialization and heterogeneous systems, approximate computing and domain-specific Energy Delay Product (EDP) optimizing technologies; and data analytics

- **DoD (HPCMP)**: Augment stable, large-scale HPC systems with targeted special-purpose or emerging computational platforms for niche and future application-space requirements; develop scalable, complex, multi-physics-based codes for critical defense applications; develop advanced cybersecurity tools and instrumentation
- **DOE/NNSA**: Investments in identified R&D critical technologies to address extreme-scale barriers via R&D collaboration with DOE/SC
- **DOE/SC**: Continued research to support data-intensive science, especially where challenges overlap those for exascale; machine learning for adaptive systems and analytics; cybersecurity
- **IARPA**: Research in superconducting supercomputing including cryogenic memory. New approaches to enable high performance computing systems with greatly improved memory capacity and energy efficiency; logic, communications and systems; development of advanced superconducting circuits and integration with memory and other components
- **NASA**: Research, explore, and exploit alternative HEC architectures such as quantum computing systems, including quantum algorithms for hard, discrete optimization problems and their mapping to and embedding on quantum architectures
- **NIST**: Measurement science for future computing and communication technologies - Quantum information science and engineering; quantum information theory (quantum algorithms, complexity: assessing the true power of quantum resources); quantum computing assessment (techniques and tools to assess the capabilities of candidate technologies); quantum technology demonstrations (evaluating feasibility of applications of quantum resources in computing, communications)
- **NOAA**: Improve speed, accuracy, integrity of data transfer for large data sets; modeling techniques for heterogeneous computing systems; big data science and tools for earth and environmental sciences
- **NSA**: Research for analytic and exploitation computing - superconducting supercomputing; quantum computing; neuromorphic computing; high performance data analytics; explore innovative solutions that meet the challenges of tomorrow for energy, productivity, and resilience of HEC systems
- **NSF**: Examine operating/runtime systems, development environments, productivity tools, languages, compilers, libraries (eXploiting Parallelism and Scalability [XPS]); quantum and biological computing; cyber-physical systems; cybersecurity (Secure and Trustworthy Cyberspace [SaTC]); networking, including integrative data cyberinfrastructure (Campus Cyberinfrastructure - Data, Networking, and Innovation [CC*DNI] contributing to campus-level data and networking infrastructure with its explicit emphasis on supporting models for potential future national-scale, network-aware, data-focused cyberinfrastructure attributes, approaches, and capabilities) and IRNC (International Research Network Connections); XSEDE – advancing the cyberinfrastructure; NSF Big Data Initiative (DIBBS, RDA, EarthCube); Open Science Grid (cyberinfrastructure, virtual organization); Advanced Manufacturing Cluster to advance manufacturing and building technologies through predictive and real-time models, novel assembly methods, and control techniques for manufacturing processes; Computational and Data-Enabled Science and Engineering (CDS&E) meta-program identifies and capitalizes on opportunities for major scientific and engineering breakthroughs through new computational and data analysis approaches
- **OSD**: Extending abstractions in the Parallel Boost Graph Library (PBGL) to support a more complete set of graph algorithms on GPUs, work to be performed at the Software Engineering Institute (SEI)

- **Productivity**
  - **DARPA**: DoD relevant benchmarks to support computing research and evaluation
  - **DoD, DOE/SC, and NSF**: Capabilities for scientific research including computational concepts, methods, and tools for discovery. Centers, institutes, and partnerships for predictive and data-intensive science; applied math and computer science challenges of data-intensive science and scientific computing at extreme scale
  - **DOE/NNSA**: Continue development of and pursue community adoption of High Performance Conjugate Gradient (HPCG) benchmark as a complement to Linpack benchmark on the Top 500 list
  - **DOE/SC and NOAA**: Explore optimal configuration for meta scheduling (Moab)
  - **NOAA**: Explore optimal configuration for job queuing management (Grid)
  - **NSF**: HEC metrics for application development and execution on high end systems; explore issues of NSF cloud operation, configuration and virtualization; technical audit and insertion services
- **Broadening impact**
  - **DoD (HPCMP):** Partner with other Federal agencies in discovery and demonstration of algorithms, tools, libraries—as well as system management, workflow, and runtime systems—that will enable DoD productivity on next-generation extreme-scale hardware
  - **NASA:** Expand the utilization of HEC in Model Based System Engineering (MBSE) and Observation System Simulation Experiments (OSSE)
  - **NSF:** CIF21 – NSF Research Traineeship in Data-Enabled Science and Engineering for software; data-enabled science and education

Planning and Coordination Supporting Request

Coordination among the HEC R&D agencies focuses on computer science advancements to improve the performance and efficiency of the current generation of HEC hardware and software as well as on avenues of fundamental research to create revolutionary new architectures and systems. The complexity of high-end hardware architectures, systems software, and supporting technologies is such that Federal program managers and researchers depend on the constant flow of information among colleagues and technical experts to keep current with developments, gain new knowledge, and share best practices and lessons learned. In addition to joint technical/planning workshops and proposal/technical reviews that HEC R&D agencies routinely conduct, the following are selected examples of the scope of interagency collaboration under each of the HEC R&D strategic priorities:

- **Extreme-scale computation**
  - **Joint workshops on extreme-scale resilience**: DoD, DOE/NNSA, and DOE/SC
  - **DOE intra-agency collaborations**: Critical R&D investments in memory, processors, storage, interconnects, systems engineering, etc.; joint development work to fully address the parallelism, power, memory, and data movement issues associated with multicore computing at the exascale level; collaboration on all aspects of the Exascale Computing Initiative (ECI) – DOE/NNSA and DOE/SC
  - **Computing MOU:** DoD, DOE/NNSA, and DOE/SC
  - **Extreme-scale R&D technologies and Modeling/Simulation Working Group:** HEC agencies
  - **Big data:** Explore synergies and convergences between HEC and the Big Data realm to ensure HEC capabilities support the many emerging data-intensive applications and domains – HEC agencies

- **New directions in HEC hardware, software, computer science, and system architectures**
  - **Quantum information theory and science**: Study information, communication, and computation based on devices governed by the principles of quantum physics – DARPA, DOE/NNSA, DOE/SC, IARPA, NASA, NIST, NSA, and NSF
  - **Superconducting (cryogenic) supercomputing**: IARPA and NSA
  - **Cloud-based HPC**: Explore supercomputing in the cloud through public and private service providers to determine applicability/efficiencies for subset of Federal HEC needs – NASA, NIH, and NSF
  - **Extreme-scale system software R&D co-funding**: DoD (HPCMP), DOE/NNSA, and DOE/SC
  - **3D stacked memory**: DOE/NNSA and DOE/SC
  - **Source code porting and scaling studies**: Collaborations for weather and climate models – NASA, NOAA, and NSF (TACC)
- **Productivity**
  - **Benchmarking and performance modeling**: Collaborate on developing performance measurement test cases with applications commonly used by the Federal HEC community for use in system procurements, evaluation of Federal HEC system productivity – DARPA, DoD (HPCMP), DOE/NNSA, DOE/SC, NASA, NSA, and NSF
  - **HEC metrics**: Coordinate on effective metrics for application development and execution on high-end systems – DoD, DOE/NNSA, DOE/SC, NASA, NSA, and NSF
  - **Meta scheduling**: Moab – DOE/SC and NOAA
- **Broadening impact**
  - **HEC hardware and software**: Facilitate access to and share knowledge gained and lessons learned from HEC hardware and software development efforts – DoD, DOE/NNSA, DOE/SC, NASA, NIST, NOAA, and NSF
  - **HEC tools**: Coordinate R&D in operating/runtime systems, development environments, productivity tools, languages, compilers, libraries – DARPA, DOD (HPCMP), DOE/NNSA, DOE/SC, NASA, NSA, and NSF
  - **HEC data challenges**: Coordinate with NITRD HCI&IM CG, LSN CG, and Big Data SSG and IWG on Digital Data – HEC agencies
  - **ASCR Committee of Visitors review of computer science program**: DOE/SC and NSF

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the HEC R&D PCA:

- **DARPA**: Research in energy-efficient technologies and architectures; data-centric technologies and architectures, including memory side processing; integrated photonic systems; unconventional computing and data representations, including a cortical processing algorithm study; embedded cooling using intra/interchip microfluidics and high conductivity materials; domain-specific acceleration in heterogeneous systems, resilience; cybersecurity; data analytics; formation of new DARPA Biological Technologies office with increased emphasis on biologically based research
- **DoD (HPCMP)**: HEC systems and software R&D in support of DoD mission priorities; modeling and simulation; user productivity; investigations into fundamentally new ways of expressing parallelism to address the strong scaling problem for current and future large scale hardware

- **DOE/SC**: Workshops for quantum computing; machine learning; storage systems and I/O; neuro-inspired computational elements; exascale tools; programming environments, operating/runtime systems; scientific workflows; release of multiple ECI-related announcements
- **NASA**: Complete the climate model downscaling experiments using high resolution regional climate models; invest in model output data analysis system software; continue to develop applications using quantum annealing processor
- **NIST**: Quantum information theory (algorithms for simulation of quantum field theories; analysis of quantum cryptographic devices); quantum computing assessment (randomized benchmarks for testing fidelity of multi-qubit gates; quantum state tomography; efficient/reliable quantification of experimental results of Bell test); quantum technology demonstrations (develop/assess quantum memory/communications interface technologies; develop specialized quantum devices, e.g., random bit generators whose values are certified to be unknown before measurement)
- **NOAA**: Continue collaborative involvement with Earth Systems Modeling Framework (ESMF); improve techniques for transitioning codes from research to operations
- **NSA**: SME collaborations (machine learning, file I/O, runtime systems, memory, and storage, etc.); system level metrics for energy, productivity, and resilience
- **NSF**: CIF21; software and data-enabled science and education (NSF Research Traineeship); cyber-physical systems; advanced manufacturing; cybersecurity (SaTC); computing workforce; high performance computing and storage services; technical audit service for gathering data and evaluating HPC; XSEDE integrating services (coordination and management service, extended collaborative support service, training, education, and outreach service); Open Science Grid (cyberinfrastructure, virtual organization)

Human Computer Interaction and Information Management (HCI&IM)

NITRD Agencies: AHRQ, DARPA, DoD Service Research Organizations, EPA, NARA, NASA, NIH, NIST, NOAA, and NSF
Other Participants: USDA, USGS, and VA

HCI&IM focuses on R&D to expand human capabilities through the use and management of data, information, and computer technologies. Such technologies include robotics, visualization agents, cognitive systems, collaborative systems, and others that support the organization and transformation of data to knowledge to action. HCI&IM research includes the collection and management of data critical to addressing national priorities, such as defense, energy, the environment, and healthcare, while also providing for public access, advances in informatics, modeling, and the technologies needed to support a broad innovation enterprise across science and engineering.

HCI&IM research spans both the technologies that enable people to access and use digital information (HCI) and those that expand the capabilities of computing systems and devices to acquire, store, process, and make accessible data and information for humans to use (IM). Transformative approaches for accessing, extracting meaning from, and displaying data remain a critical need because the volume, variety, and velocity of data are quickly overtaking the technical capabilities to process, manage, and analyze it. The Federal Government generates and maintains the world's largest digital collections of science and engineering data, historical records, health information, and scientific and other types of archival literature. Rapid knowledge discovery requires next-generation methods, technologies, and tools that integrate and efficiently manage massive stores of streaming, distributed, heterogeneous information while integrating the human in the discovery process. Such capabilities are essential for U.S. economic growth and technological innovation.

President's FY 2016 Request

Strategic Priorities Underlying This Request

Strategic priorities in HCI&IM include:

- **Data visualization:** Directions for research to enable the enhancement of visualization tools used in collaborative and multi-user environments to better enable decision making and manipulation of large data sets through increased usability
- **Human-system engagement and decision-making systems**:
    - **New methods** to make large, diverse, and streaming data sets meaningful to analysts and decision makers in a timely way
    - **Personalization** that requires individual human-performance modeling and multimodal interfaces, including a crosslink to cognitive and perceptual process modeling, task type, and measurement
    - **Human-autonomy teaming** that enables seamless interaction between humans and systems for understanding and decision making, with reliance on shared awareness and trusted interaction
- **Information integration**:
    - **Decision support systems** provide mechanisms for sifting through large, complex data sets to identify alternative strategies from the data that, without computational analysis, would strain human cognitive capabilities
    - **Information management systems** enable individuals and organizations to create, share, and apply information to gain value and achieve specific objectives and priorities

- **Standards** provide a way to ensure effective human system interaction and establish the basis for interoperability essential to integrating and managing data

- **Information infrastructure**: A robust, resilient national digital data framework for long-term preservation and accessibility of electronic records as well as expanding data and records collections

Highlights of the Request

The HCI&IM agencies report the following areas as highlights of their planned R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **From big data to new knowledge and action**: Analysis R&D requires not only new computing research in models, algorithms, and tools to accelerate scientific discovery and productivity from heterogeneous, ultra-scale data stores, but also development of innovative, multidimensional approaches to highly complex data. For complex data, new ways should be developed to enable the intuitive display of complex interactions and mechanisms that enhance both discovery and use of data, as well as effective analytical products for decision makers and the public – AHRQ, DARPA, DoD Service research organizations, EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies

- **Human engagement and decision-making**: Design effective HCI and systems integration that provide personalization. This requires human-performance modeling, multimodal interfaces, and mechanisms for distributed collaboration, knowledge management, virtual organizations, and visual environments. There is a crosslink to cognitive and perceptual process modeling and measurement. Expand virtual reality technologies for simulation and training as well as biometric and voting systems – DoD Service research organizations, EPA, NASA, NIST, NOAA, and NSF

- **Effective stewardship of science and engineering data**: This effort will maximize the value gained from current and previous Federal investments but will require additional research in providing for life-cycle stewardship over time. Research foci include personalized access to information, as well as federation, preservation, curation, data life-cycle stewardship, and analysis of large, heterogeneous collections of scientific data, information, and records. A persistent issue is the need for fault-tolerant, scalable management of information input and output in light of new system architectures – EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies

- **Information integration, accessibility, and management**: Multiple advances are required in technologies, system architectures, and tools for optimized, scalable ingest and processing for high-capacity data integration (especially of Geographic Information System [GIS] and spatio-temporal data), management, exploitation, modeling, and analysis. In addition, investigation continues in cloud-based infrastructures to efficiently gain distributed access to data resources utilizing new ontologies and metadata formats for discovery – AHRQ, DARPA, EPA, NARA, NASA, NIH, NIST, NOAA, and NSF

- **Earth/space science data and information systems**: These efforts enable multiagency access to and use of Federal scientific data resources through Web-based tools and services (e.g., remote visualization) that exploit advances in computer science and technology – EPA, NASA, NOAA, NSF, and other agencies

- **Health information technologies**: NITRD's Health IT R&D CoP is developing guidance for R&D in this area. Research needs that have been identified include expansion of clinical decision-support systems, development of more effective use of electronic health records and data, and defining national health information and device interoperability standards – AHRQ, FDA, NIH, NIST, NSF, ONC, and other agencies

- **Information search and retrieval**: New research methods and tools are necessary for evaluation and performance measures of information-discovery technologies, as well as relevance feedback. Current focus areas include legal discovery, recognition of opinion, and patent search, as well as domain-specific search and machine reading of records – DARPA, NARA, NIST, and NSF

- **Cognitive, adaptive, and intelligent systems**: Algorithmic and multidisciplinary research is designed to discover the cognitive, perceptual modeling for joint cognitive systems design; autonomy, trustworthiness, and reliability of automated systems; engineered intelligence and adaptability; robotics, human-robot teaming; automated computational intelligence; affective computing – DARPA, DoD Service research organizations, NARA, NASA, NIST, and NSF
- **Multimodal language recognition and translation**: Improve multilingual language technology performance in areas of speech-to-text transcription and text-to-text transcription. A goal is to provide spontaneous two-way communications translation, machine reading, text retrieval, document summarization/distillation, automatic content extraction, and speaker and language recognition through multimodal interfaces – DARPA, DoD Service research organizations, NARA, NASA, NIST, and NSF

Planning and Coordination Supporting Request

Although the HCI&IM portfolio includes a broad range of enabling technologies, the current focus of coordination among the agencies is the overriding challenge of ultra-scale, heterogeneous data: how to manage it, enable interoperability and usability, and develop new infrastructures and tools that broaden access and exploration to a wider range of end users. The following HCI&IM collaborations seek to forward this agenda:

- **Foundations of visualization and analysis**: This provides a multiagency mechanism for coordination of research in feature extraction for anomaly detection, integration of multiple types of data and records at scale or format, the use of visualization as an interface, and biomedical imaging. The follow-on activities in the "Frontiers of Visualization" meeting series will focus on research needs in various knowledge areas – AHRQ, EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies
- **Science and Science Innovation Policy Interagency Task Group**: Coordination on Federal science policy issues and metrics – HCI&IM agencies and others
- **Biodiversity and Ecosystem Informatics Task Group**: The group provides an ongoing Federal point of contact and body for cooperation, with a focus on aspects of environmental, natural resources, and sustainability as outlined in the President's Council of Advisors on Science and Technology (PCAST) July 2011 report *Sustaining Environmental Capital: Protecting Society and the Economy*[17] – DoD, DOE/SC, EPA, Interior, NASA, NIH, NOAA, NSF, and other agencies
- **Earth/space science, climate, and weather**: Agencies focus on cooperative activities in providing interoperable data (including through the Big Earth Data Initiative), multidimensional models, and tools for better understanding and prediction based on the growing corpus of observational and experimental data – DoD Service research organizations, EPA, NASA, NOAA, NSF, and other agencies
- **National Robotics Initiative**: Innovative robotics research and applications that emphasize the realization of co-robots acting in direct support of, or in a symbiotic relationship with, human partners – NASA, NIH, NSF, and USDA
- **Information access, management, and preservation**: Multiple agencies have participated in the IWG on Digital Data (IWGDD) and the Task Force on Public Access to Scholarly Publications (PASP). Topics for follow-on consideration and coordination include new policy development and identification of existing standards for interoperability, such as the Digital Preservation Interoperability Framework International Standard (DPIF). Agencies have also been called to meet requirements identified in the Presidential Records Management Directive focusing on electronic recordkeeping – EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies

[17] *Sustaining Environmental Capital: Protecting Society and the Economy*. July 2011, PCAST: http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_sustaining_environmental_capital_report.pdf

- **Usability**: People are the ultimate users of information. Usability research draws input from the social and behavioral sciences and informs the design and evaluation of technical solutions with the goal of ease of use. Research areas include health IT, security, voting, biometrics systems, and decision-support systems – AHRQ, NIST, and NSF

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the HCI&IM PCA:

- **AFRL**: Technologies to enhance the decision making of RPA operators, ISR analysts, and CYBER personnel to include natural, adaptive, trusted information management and decision-support tools; effective teaming of distributed operators and increasingly autonomous systems; and live, virtual, constructive immersive training and learning management
- **AHRQ**: Quality measurement and improvement; healthcare decision making; patient and clinician information needs; U.S. Health Information Knowledgebase; evidence-based practice center reports
- **DARPA**: Human prosthetics interactions; visualization and analysis of Big Data; new ways of conducting domain-specific queries and interacting with the World Wide Web; new visual search methods for searching the pixel content of massive amounts of photos and videos; methods for computer systems to understand the context of human commands; interfaces for visualizing and conducting cyber operations; and systems that can read and extract potential causal models from massive volumes of diverse text data for human confirmation and analysis
- **EPA**: Databases for computational toxicology; scientific information management (tools, best practices for management, accessibility of complex EPA data sets); distributed environmental applications; and air quality forecasting
- **NARA**: Global-scale, open source, next-generation technologies, architectures, and services enabling effective, sustainable management, intellectual control, and access to nationally distributed billion-file-and-larger scale, complex digital object collections
- **NASA**: Earth Science Data collaborative systems; basic and applied research in human performance; decision-support technologies for NextGen; multimodal interface research; research on advanced tools for discovering tools and services, and developing and preserving provenance of data products and information
- **NIH**: Collaborative Research in Computational Neuroscience (CRCNS) - Innovative Approaches to Science and Engineering Research on Brain Function; Big Data Centers of Excellence; Analysis of Genome-Wide Gene-Environment (GxE) Interactions; focus areas include decision making for patients and clinicians, natural language understanding, organization and retrieval of health-related information by consumers, visualization and mapping of heterogeneous data for clinical researchers, support for healthy behaviors, and device interfaces
- **NIST**: Biometrics evaluation, usability, and standards (fingerprint, face, iris, voice/speaker); multimedia evaluation methods (video retrieval, audio and video analysis); measurement, evaluation tools for 3D shape searching; data preservation and data science metrology; usability and user-centered research for cybersecurity infrastructure, health information technology, cloud computing, voting systems, and privacy; manufacturing supply chain informatics; standards for manufacturing robots; engineering informatics sustainability; computational biology; mathematical knowledge management
- **NOAA**: Technologies for real-time weather/climate data in multiple formats for scientists, forecasters, first responders, and citizens; remote visualization via N-Wave, new high-definition devices; disaster planning, mitigation, response, and recovery

- **NSF**: Through academic R&D, NSF supports CIF21 as well as programs in support of information privacy, data and open publication access, ubiquitous networked data environments, human-computer partnerships, socially intelligent computing, understanding the science of information, cognition mechanisms in human learning, and remote access to experimental facilities

Large Scale Networking (LSN)

NITRD Agencies: AFRL, AHRQ, DHS, DoD (CERDEC, DREN, HPCMP), DOE/SC, NASA, NIH, NIST, NOAA, NSA, NSF, ONR, and OSD

LSN members coordinate Federal agency networking R&D in leading-edge networking technologies, services, and enhanced performance. This includes programs in fundamental networking research and architectures, future Internet architectures, wireless networks, software defined networks, heterogeneous multimedia networks, testbeds, and end-to-end performance and performance measurement. Program coordination also spans network security, privacy, and identity management; dynamic inter-domain networking; public service networks; the science and engineering of complex networks; network infrastructures for advanced discovery environments; network-enabling technology; networking education, training, and outreach; and cyberinfrastructure for scientific and applications R&D. The results of this coordinated R&D, once deployed, assure that the next-generation Internet will be scalable, reliable, and flexible.

President's FY 2016 Request

Strategic Priorities Underlying This Request

The missions of the LSN agencies, though varied, all require ultra-high-speed communications, ultra-scale data-transfer capabilities, and virtualization and collaboration capabilities with demanding constraints on end-to-end performance, security, privacy, reliability, resilience, and availability. The advanced Federal research networks support national security and privacy needs and transfer data among the world's leading science centers and observational systems on the ground, on the seas, in the air, and in space. Each year, the LSN agencies identify a small number of priority areas in which focused research collaboration will promote advances in networking that address these needs and benefit all. The big data testbed, for example, identifies architectures and deploys best practices for transport of big data in support of advanced science applications. LSN collaborative activities for 2016 will focus on:

- **Enabling end-to-end big data applications**: Build on the big data testbed demonstrations of FY 2015 and expand the networking support of big data transfers, extend leading-edge network technology for big data, monitor the network performance, and work with application users to improve end-to-end throughput, reliability, and security of big data transfers
- **Operational capabilities**: Identify approaches, best practices, and testbed implementations for Software Defined Infrastructure (SDI), Software Defined Networking (SDN), and SDN Exchanges (SDXs), tactical communications and emerging network technologies (e.g., dynamic ad-hoc, multi-hop, secure, robust wireless networks and virtual/data-centric environments), low probability of detection and anti-jam networks, identity management, distributed computing, cloud computing, collaboration capabilities, spectrum management, IPv6, DNSSEC, science DMZ, Trusted Internet Connections (TICs), and perfSONAR
- **Optical networking**: Coordinate the development and deployment of dynamic optical networking, SDN, and virtual and distributed computing infrastructure and architecture to support leading-edge science applications, multiple 100 Gbps connectivity for large data flows, and trans-Atlantic 100 Gbps lambdas

Highlights of the Request

The LSN agencies report the following topical areas as highlights of their planned networking R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **Network architectures and protocols for future networks (FIA-NP, GENI, NeTS, CIF21)**: Develop and test network architecture concepts to enable reliable, secure, flexible, and dynamic networking capabilities for heterogeneous, hybrid, and peer-to-peer networks; support sustainable environments, efficient Size, Weight, and Power (SWaP) networking, virtualization at scale, and mobile hotspots – AFRL, CERDEC, DoD (HPCMP), DOE/SC, NASA, NIST, NSF, ONR, and OSD

- **Big data networking**: Develop and test terabit-plus end-to-end architecture and protocols for big data (integrated with storage, applications, and computational resources), e.g., science DMZ, SATCOM – DOE/SC, NASA, NOAA, NSA, and NSF
- **SDI, SDN, and SDX technology**: Develop, deploy, and operate dynamic, secure, inter-domain, layers 1, 2, and 3 operational and virtualized networking capability – DoD, DOE/SC, NASA, NIST, NSA, and NSF
- **Wireless networking**: Develop standards and tools enabling better interconnectivity, seamless multi-domain, heterogeneous, and layer interoperability; electronic warfare/communications coexistence and management for wideband (e.g., SWaP reduction, data fusion, heterogeneous interfaces, spectrum management and efficiency, sensing and sharing, mobile hotspots, constraints and efficiency, low probability of detection, and anti-jam); robust, secure, resilient, dynamic, mobile, Delay-Tolerant Networking (DTN), spread-spectrum, Long Term Evolution (LTE) Advanced, WiFi, WiMAX, airborne, and sensor networks – AFRL, CERDEC, NASA, NIST, NSA, NSF, and ONR
- **Experimental network facilities**: Provide testbeds at differing scales, promote cooperation, and test advanced applications on DOE/SC's Advanced Networking Initiative (ANI) (100/400 Gbps), NSF's Global Environment for Networking Innovations (GENI), international 100+ Gbps, and other R&D testbeds, to demonstrate performance at scale of new architectures (e.g., SDN), end-to-end applications (e.g., US Ignite), and protocols – DOE/SC, NASA, NIST, NOAA, NSA, and NSF
- **Strategic technologies for networking**: Provide basic research, development, and demonstration of new and heterogeneous technologies for robust, secure, private, reliable, evolvable wired and wireless networking, underwater communications, autonomous dynamic ad hoc routing infrastructure, tactical networking, medical devices, and assistive technologies – CERDEC, DOE/SC, NIST, NSA, NSF, and ONR
- **Advanced discovery environments**: Provide grid and cloud services infrastructure that supports extreme-scale scientific knowledge discovery; provide security, management, and support for multi-domain collaborations, cyber-physical systems, data distribution and management, visualization, software stacks for large-scale scientific collaborations, high-bandwidth implementation, standards for smart grid interoperability, and testbeds; support for Open Science Grid (OSG) – DOE/SC, NASA, NIH, NIST, NOAA, NSA, and NSF
- **Computational research infrastructure (CC*DNI, IRNC, ESnet, N-Wave, science DMZ, Hawaii and Alaska connectivity, NIH medical database access)**: Provide networking to support U.S. and international research communities for networking research, large-scale data flows, end-to-end throughput, real-time networking, health science, clinical support, and applications across all science disciplines – AHRQ, DoD (HPCMP), DOE/SC, NASA, NIH, NIST, NOAA, and NSF
- **Energy aware and efficient networks**: Develop energy efficient technology and architectures for end-to-end big data applications, ad hoc mobile wireless and sensor networking, SWaP-efficient networking, and modeling for economic sustainability – AFRL, CERDEC, DOE/SC, NSA, NSF, and ONR
- **End-to-end network management**: Enable cross-domain end-to-end performance measurement for advanced networking; enable autonomous secure management; provide tools for and implement performance Services-Oriented Network Architecture (perfSONAR) – CERDEC, DOE/SC, NASA, NIST, and NSF
- **Network security and privacy research**: Develop technologies for detection of anomalous behavior; standards, modeling, and measurement to achieve end-to-end security over wireless networks and heterogeneous, multi-domain networks and infrastructure; critical infrastructure protection; DTN;

trustworthy networking; privacy, confidentiality, authentication, policy, cryptography – AFRL, CERDEC, DOE/SC, NASA, NIH, NIST, NSA, NSF, and ONR

- **Security implementation (protected SATCOM, cybersecurity defenses, IPv6, DNSSEC, DTN, TICs)**: Develop and implement near-term mandated capabilities – DOE/SC, DREN, NASA, NIH, NIST, NSA, and NSF
- **Complexity in networking**: Develop concepts, methods, architectures, protocols, and measurement for modeling networks as complex, autonomous, and dynamic systems – DOE/SC, NIST, and NSF
- **Public-safety networking, disaster recovery, and crisis management**: Provide Disaster Information Management Research Center (DIMRC), public-safety communications, implant communication system – NIH (NLM) and NIST

Planning and Coordination Supporting Request

The LSN agencies have extensive experience working through interagency and private-sector partnerships to interconnect and extend the capabilities of federally supported research networks. For example, by engaging participants from academia, industry, national labs, and international networking groups, LSN's Joint Engineering Team is able to coordinate efforts at the global level to resolve technical networking issues and develop collaborative testbeds for exploring advanced technologies at scale. The following are ongoing LSN coordination activities:

- **Big data networking and demonstrations**: Networking and demonstrations for extreme-scale science and data flows; experimentation, network management, perfSONAR deployment; DTN; experimental design for complex systems; network performance measurement; network security; and GENI, OpenFlow, US Ignite, and SDN testing – LSN agencies
- **Infrastructure cooperation**: National and trans-oceanic connectivity and performance measurement, TICs, TIC Access Providers (TICAPs) – DOE/SC, DREN, NASA, NOAA, and NSF
- **Application development**: GENI, US Ignite – DOE/SC, DREN, and NSF
- **Multiagency workshops**: Software Defined Networking Planning; Future infrastructure needs for large-scale outdoor wireless experimentation; Mid-Scale Cyberinfrastructure Control – DoD, DOE/SC, NSF, and other LSN agencies
- **400 Gbps/terabit networking research** – DOE/SC, NSF, and other LSN agencies
- **Inter-service collaboration (DoD)**: Research on robust, reliable, secure wireless and heterogeneous networking; spectrum access and management; SDN; DTN; dynamic spectrum access; near-real-time networking; SATCOM; cybersecurity; services for federation, management, information, discovery, and secure delivery; mobile hotspots; resilient tactical networks – AFRL, CERDEC, and ONR
- **Software Defined Infrastructure –** Testing of SDN and SDX applications in at-scale testbeds – DOE/SC, DREN, NASA, NIST, NSA, and NSF
- **Internet infrastructure protection, anti-DDoS technology –** DHS, NIST, and NSA
- **End-to-end performance measurement, metrics –** DREN, DOE/SC, NASA, NIST, and NSA
- **Public safety communication research** – ITS, NIST, and NTIA
- **Information exchange**: Multiagency participation in review panels, informational meetings, principal investigator (PI) meetings; coordination among program managers; and joint JET, DOE Energy Sciences Network Steering Committee (ESSC) and Internet2 Joint Techs Meetings – AFOSR, DOE/SC, NASA, NIST, NSA, NSF, and ONR

- **Coordination by LSN Teams**
  - **Joint Engineering Team (JET)**: Coordination of end-user requirements, science user interfaces, engineering of research networks and testbeds (JETnets); networking for advanced demonstrations; end-to-end big data transport and storage networks; security best practices, application testbeds (DNSSEC, IPv6, performance measurement), TIC/TICAP coordination; inter-domain and end-to-end metrics, monitoring; tool sharing and exchange; international coordination; and transit and services cooperation – DOE/SC, DREN, NASA, NIH, NIST, NOAA, NSA, NSF, and ONR
  - **Middleware And Grid Interagency Coordination (MAGIC) Team**: Research for evolution of distributed computing, cloud and grid computing services, middleware; cloud and grid standards and implementation status (XSEDE, Open Science Grid); best practices for resource architecture, access, and management; security and privacy, e.g., identity management; and international coordination – DOE/SC, NASA, NIST, and NSF

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the LSN PCA:

- **AFRL**: Reliable wide-band line-of-sight and beyond links, assured access communications, link survivability in operational environments, adaptive and resilient information services, heterogeneous networks, secure multidomain network services, enterprise-to-tactical information services, multi-mission software defined RF, multi-level security routing, secure tactical intranet, information management enabled sensor tasking and control
- **AHRQ**: Personal Health Information Management (PHIM) tools; with CMS, ONC, NIH (NLM) - United States Health Information Knowledgebase (USHIK)
- **CERDEC**: Protected SATCOM, SWaP reduction, communications/electronic warfare co-existence, defensive cyber operations, multi-layer and inter-domain routing, SDN, DTN, dynamic spread spectrum, communications in a contested electronic warfare environment, SATCOM extension to tactical maneuver platforms, increased bandwidth, interference resistance, dynamic spread spectrum
- **DOE/SC**: SDI research, SDN networking, extreme-scale scientific knowledge discovery and software sustainability research, understanding applications on complex networks, multiple 100 Gbps end-to-end testing with science applications, 400 Gbps networking, big data networking demonstrations, trans-Atlantic 100 Gbps lambdas, couple data generation sources with data analysis via networks, cutting-edge user network infrastructure and support, science DMZ, open exchange point (layers 1,2,3)
- **DREN**: Next generation networking and testing for applications (100G, SDN, US Ignite); implement network services (IPv6, DNSSEC, TICs, science DMZ, Network Time Protocol [NTP], Video Teleconferencing [VTC], performance measurement); develop/deploy cybersecurity defenses (intelligent agent sensor networks, Jigsaw and Assured Compliance Assessment Solution [ACAS] tools); advanced networking (DREN III); and network high-speed access to Alaska and Hawaii
- **NASA**: Access to computing facilities, DTN, science DMZ, 40/100G networking and testbed, SDN, SDX, Network Functions Virtualization (NFV), cloud services, performance measurement, TIC, Information Technology (IT) Infrastructure Integration Program (I3P), security and intrusion protection, IPv6
- **NIH**: Advanced networking for health science research, clinical needs and disaster management, networking for biomedical computing (Big Data to Knowledge [BD2K]), connectivity/access for National Center for Biotechnology Information (NCBI), TICs, 100G infrastructure

- **NIST**: Next generation network technologies and architectures, develop measurement science and apply to network systems, public safety communications, spectrum efficient and public safety communications, science of complex information systems, cloud computing standards and measurement, standards for data accessibility, data science measurement and benchmarking, networked cyber physical systems, metrology for new security paradigms, internet infrastructure protection
- **NOAA**: N-Wave integration of and access to HPC and data centers, X-Wave external peering network, TICAP resiliency, TIC interagency cooperation, cybersecurity, science DMZ, shared network infrastructure including access to Alaska and Hawaii
- **NSA**: SDN (security focus), cloud computing (Accumulo), low SWaP, Tbps networking, cyber defense at scale, extreme data transport, critical infrastructures, DTN
- **NSF**: Innovative networking architectures to support application domains (NeTS, enterprise, core, Tbps optical, wireless, cellular peer-to-peer, smart grids, compute grids, clouds, data centers networking), leverage and advance new networking technologies; Future Internet Architecture – Next Phase (FIA-NP) to demonstrate prototype systems, architecture, security; Global Environment for Networking Innovations (GENI) program (WiFi, WiMAX, deploy GENI racks); NSFCloud program (infrastructure, academic/industry interaction); US Ignite application development; Campus Cyberinfrastructure – Data, Networking, and Innovation (CC*DNI) program (end-to-end access to dynamic network services, innovative networking, identity and access management, regional centers); International Research Network Connections (IRNC) program (international multi-Gbps, U.S. and Europe connectivity with Africa, SDN-based experiments, >200 Gbps trans-Atlantic connectivity); Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21) program (integrated scalable cyberinfrastructure across all science and engineering disciplines); Cyber-Innovation for Sustainability Science and Engineering (CyberSEES) program (sustainability research, energy efficiency, disaster resilience)
- **ONR**: Spectrum and energy efficient communications; tactical communications (high-bandwidth optical, dynamic ad-hoc multi-hop wireless, dynamic spectrum access, underwater communications for sensors); underwater communications, multi-commodity flow optimization, network management and optimization, SDN (government-developed alternative to Cisco routers), Dynamic Tactical Communications Networks (DTCN)

Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)

NITRD Agencies: AFOSR, ARO, DHS, DOE/NNSA, DOE/SC, NASA, NIH, NIST, NSF, NRL, ONR, and OSD
Other Participants: BLS, ED, IARPA, and USDA

Research activities funded under the SEW PCA focus on the co-evolution of IT and social, economic, and workforce systems, including interactions between people and IT and among people developing and using IT in groups, organizations, and larger social networks. Collaborative science concerns are addressed including understanding and improving the effectiveness of teams and enhancing geographically distributed, interdisciplinary R&D to engage societal concerns, such as competitiveness, security, economic development, and wellbeing. Workforce concerns are addressed by leveraging interagency efforts to improve education outcomes through the use of learning technologies that anticipate the educational needs of individuals and society. SEW also supports efforts to speed the transfer of R&D results to the policymaker, practitioner, and IT user communities in all sectors.

President's FY 2016 Request

Strategic Priorities Underlying This Request

Priorities in SEW reflect the sweeping socio-technical transformations occurring as a result of 21st century life in an increasingly networked society. From crowdsourcing to e-science to cyberlearning, new forms of social collaboration and problem-solving increasingly leverage networked, online environments. In cyberspace, thousands voluntarily contribute time and intellectual resources for collective tasks, such as writing open-source software, classifying galaxies, and identifying words in non-machine-readable text. Global multidisciplinary teams connected through cyberinfrastructure play a central role in addressing societal needs, such as developing economical solar power, mitigating environmental disasters, delivering new medical interventions, and maintaining our national security. A new era of human-machine partnerships is emerging, but we do not yet understand how to harness these novel forms of collective action most effectively. In this new era, developing cyber-capable citizens is also critical – from the ability to use digital capabilities wisely and effectively, to the IT skills and knowledge needed in the advanced technical workforce of tomorrow. It is imperative that the general population be able to understand the challenges in complex systems, such as in healthcare information infrastructures, e-commerce, and cyberlearning, and to balance trade-offs with respect to privacy, security, and reliability. SEW priorities exemplify the scope of these concerns among the NITRD agencies. Many SEW activities involve extending understanding and applications of IT to help people learn, conduct research, and innovate more effectively. Key focus areas include:

- **Collaboration**
  - **Increase fundamental knowledge**: Advance understanding of how to efficiently and effectively manage, conduct, fund, and reward science teams collaborating with and via cyberinfrastructure by developing evidence-based approaches for managing, conducting, funding, and studying effective and efficient cross-disciplinary collaborative research
  - **Integrated multidisciplinary research**: Support empirical research, development, and education to improve capabilities for meeting societal challenges using a multidisciplinary systems-based approach to understand, predict, and react to changes in the linked natural, social, and built environment – especially in climate change, energy, health, education, and security
  - **Research networking and profiling tools**: Advance our understanding of the complex and increasingly coupled nature of scientific research to facilitate collaboration among Federal agencies and to increase the cross-fertilization of ideas and collaborative effectiveness and efficiency within and across agencies

- **Education**
  - **Transform science teaching across educational settings**: Integrate Science, Technology, Engineering, and Mathematics (STEM) education R&D and IT innovations to improve learning in science and engineering disciplines. Bring new evidence-based practices, content, knowledge, and real-world applications to more learners. Provide evidence-based professional development and support to STEM educators in the classroom to improve STEM instruction and retain effective teachers
  - **Cyberlearning**: Promote understanding and support for effective IT-enabled learning in all educational settings to enhance learning anytime in any location. Provide learning that is personalized and tailored to the needs of diverse learners. Transform science teaching across educational settings
  - **Computational competencies for everyone**: Explore how the nature and meaning of computational competence can be incorporated into K-12, informal, and higher education
  - **IT education and training**: Develop innovative approaches to broaden interest and participation in 21st century IT careers, including information assurance, computer security, predictive science, and multi-core computing technologies
  - **Preparing effective STEM teachers**: Recruit, prepare, and support talented individuals with strong content knowledge to become effective STEM teachers; engage STEM teachers in influencing the design and development of educational technologies (EdTech) and in understanding evidence on learning styles to use to teach effectively in IT-enabled learning settings that span beyond the classroom
- **Social computing**
  - **Increase fundamental knowledge**: The NITRD Social Computing Team is focusing on understanding the wide range of systems that support interactions among large numbers of individuals at different scales, but differ along a number of dimensions: the topology and goals of interaction, media richness, and degree of virtualness. Research is needed to understand how to design such systems and make them effective, rewarding, and sustainable; to understand the dynamics of online social systems; and to understand the technical effects that emerging social phenomena empowered by ubiquitous online services have on specific areas such as security, privacy, health, and scientific discovery

Highlights of the Request

The SEW agencies report the following topical areas as highlights of their planned R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **Collaboration**
  - **Multidisciplinary centers, institutes, communities and platform**: Support collaborative activities to advance a field or create new directions in research or education by providing a platform to enable coordination of research, training, and educational activities across disciplinary, organizational, geographic, and international boundaries. Create centers to coordinate multiyear activities addressing national challenges such as big data, translational sciences, energy efficiency, environmental sustainability, advanced communication, transportation, learning, and healthcare systems – DOE/NNSA, NASA, NIH, and NSF
  - **Cyber-human systems**: Focus on the co-evolution of social and technical systems to create new knowledge about human-machine partnerships and of the purposeful design of such systems, including e-science collaboration tools, human-robot partnerships, cyber-physical systems, advanced manufacturing, cyber-enabled materials, manufacturing and smart systems, and handling big data – NASA, NIH, and NSF

  - **Collaboration data**: Explore agency and research datasets on scientific collaboration studies and expand access to all datasets including sociometric badges, social media, and trace data. Leverage, analyze, share, and crosslink datasets to measure outcomes

- **Education**
  - **Advanced learning technologies**: Understand advanced learning technologies that have demonstrated potential to transform STEM teaching and learning at all levels across all societal settings; understand technologies that can contribute to a highly interdisciplinary technical STEM workforce; enable new avenues of STEM learning with novel, collaborative, and global learning experiences for students, the general public, and the emerging IT workforce; advance the Nation's ability to study the learning process discretely and rapidly deploy new understandings and adaptive and assistive resources in education to broaden participation of all Americans in STEM R&D, including returning disabled veterans – ED and NSF
  - **Cybersecurity education**: Bolster formal education programs to focus on cybersecurity and STEM – ED, NIST, and NSF
  - **Cybersecurity workforce training and professional development**: Intensify training and professional development programs for the existing cybersecurity workforce – NIST, NSF, and other agencies
- **Social computing**
  - **Social computing**: Collect information about existing Social Computing programs and initiatives across Federal agencies to determine if there are overlaps and collaboration opportunities and to identify gaps for multiagency R&D funding – NASA, NSF, and other agencies

Planning and Coordination Supporting Request

The SEW Coordinating Group (SEW CG) continues to pursue opportunities for expanded interagency collaborations to improve IT education and workforce training, team science, and social computing. Over the coming year, the SEW CG plans to engage in a series of workshop discussions to develop strategic plans and associated agendas for its three teams: SEW-Collaboration, SEW-Education, and Social Computing. The SEW CG also promotes interactions between IT researchers, practitioners, and government policymakers. The SEW-Collab Team plans to engage agencies in developing best practices for planning, awarding and evaluating large collaborative proposals. The SEW-Ed Team continues to track the reorganization of Federal STEM education programs, as outlined in the Federal STEM Education 5-Year Strategic Plan.[18] The Plan identifies NSF, ED, and the Smithsonian Institution as the lead agencies for Federal STEM education programs. In the upcoming year, the Social Computing Team plans to focus on and coordinate efforts that emphasize crisis management, crowdsourcing, cognitive security, privacy, and social sensors.

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the SEW PCA:

- **DoD**: Meet the DoD's requirements for a diverse, world-class STEM talent pool with the creativity and agility to meet national defense needs; ensure the implementation of the DoD STEM Strategic Plan aligns with the DoD's Strategic Workforce Plan and the NSTC Committee on STEM Education 5-Year Strategic Plan; assess and leverage DoD STEM investments

[18] *Federal Science, Technology, Engineering, and Mathematics (STEM) Education 5-Year Strategic Plan*, May 2013, NSTC: http://www.whitehouse.gov/sites/default/files/microsites/ostp/stem_stratplan_2013.pdf

- **DOE/NNSA**: Critical-skills development of university participants in the Advanced Simulation and Computing (ASC) Alliance Program and training of next-generation computational scientists in the DOE Computational Science Graduate Fellowship program
- **DOE/SC**: Maintain a healthy pipeline of computational scientists equipped and trained to address DOE's mission needs, including advances in exascale computing, by supporting the Computational Science Graduate Fellowship program
- **NIH**: Promote the use of technologies that improve educational outcomes of both trainees and established scientists by facilitating the efficient acquisition of knowledge and skills. Increase knowledge of scientific workforce dynamics in areas critical to advancing the NIH mission by developing evidence-informed policy decisions
- **NIST**: Designated lead agency for the National Initiative for Cybersecurity Education (NICE) to promote coordination of existing and future activities in cybersecurity education, training, and awareness to strengthen the overall cybersecurity posture of the U.S. by accelerating the availability of educational and training resources designed to improve cybersecurity behavior, skills, and knowledge
- **NSF**: Advance new modes of collective intelligence (e.g., social, participatory, and intelligent computing) while also ensuring that human values are embedded in these emerging systems and infrastructures; support the human capital essential for advances across all disciplines by linking key areas of educational investments in HEC, data, education, software, virtual organizations, networking, and campus bridging; broaden participation in computing by underrepresented minorities; support faculty, graduate, and undergraduate fellowships, traineeships, and junior faculty; promote digital gaming in education; Discovery Research K-12 (DRK-12) program for significant and sustainable improvements in STEM learning, advance STEM teaching, and contribute to improvements in the Nation's formal education system

Software Design and Productivity (SDP)

NITRD Agencies: AFRL, DHS, DOE/SC, NASA, NIH, NIST, NOAA, NSF, ONR, and OSD
Other Participants: FAA, FDA, and NRC

A computational revolution is transforming industry and society, driven by software operating and interacting with physical, personal, and social environments. Software and the possibilities for computational behaviors are transforming every facet of every industry. Products that are not computational are dependent upon computationally intensive simulation-based engineering and science (SBE&S) or manufactured by computational machinery. Pervasive computational behaviors present enormous opportunities for industry and society but also pose significant challenges. Current technology works quite well in many familiar domains of modest scale, so long as the error-prone characteristic of the software is accepted. The cost of these errors includes increased vulnerability of the software to cyber attack and the waste of users' time and effort required to avoid and mitigate the errors. However the world is changing in a big way (e.g., autonomy, biocomputing, multicores, social networking, big data, thought-driven prosthetics, programmable matter) and current software technology is not advancing sufficiently to keep up. Meeting these challenges requires solving the intellectually deep, difficult, and important problems in the science, mathematics, and engineering of computational behaviors, information processes, and software representations.

The SDP R&D agenda spans the science and the technology of software creation and sustainment (e.g., development methods and environments, V&V technologies, component technologies, languages, and tools) and software project management in diverse domains. R&D will advance software engineering concepts, methods, techniques, and tools that result in more usable, dependable, cost-effective, evolvable, and sustainable software-intensive systems. The domains cut across information technology, industrial production, evolving areas such as the Internet, and highly complex, interconnected software-intensive systems. The core SDP R&D activities are software productivity, software cost, responsiveness to change, and sustainment. The success of these activities can have a major beneficial effect on high-confidence systems because such systems are critically dependent upon the quality of the software and on the many companies producing software-reliant products.

President's FY 2016 Request

Strategic Priorities Underlying This Request

Complex software-based systems today power the Nation's most advanced defense, security, and economic capabilities. Such systems also play central roles in science and engineering discovery and, thus, are essential in addressing this century's grand challenges (e.g., low-cost, carbon-neutral, and renewable energy; clean water; next-generation health care; extreme manufacturing; space exploration, etc.). These large-scale systems typically must remain operational, useful, and relevant for decades. The involved agencies are working to identify and define the core elements for a new science of software development that will make engineering decisions and modifications transparent and traceable throughout the software lifecycle (e.g., design, development, evolution, and sustainment). A key goal of this science framework is to enable software engineers to maintain and evolve complex systems cost-effectively and correctly long after the original developers have departed. This new science of software development will also benefit the many companies producing software-reliant products that comprise an increasing portion of the economy. The following areas are research priorities:

- **Research to rethink software design**: From the basic concepts of design, evolution, and adaptation to advanced systems that seamlessly integrate human and computational capabilities, including:
    - **Foundational/core research on science and engineering of software:** Develop new computational models and logics, techniques, languages, tools, metrics, and processes for developing and analyzing software for complex software-intensive systems (e.g., a fundamental approach to software engineering

that can provide systems that are verifiably correct, assured, efficient, effective, reliable, and sustainable)

- **Next-generation software concepts, methods, and tools:** Reformulation of the development process, the tool chain, the partitioning of tasks and resources; open technology development (open-source and open-systems methods); technology from nontraditional sources; multidisciplinary and crosscutting concepts and approaches; and next-generation software concepts, methods, and tools will be needed for emerging technologies such as multicore, software-as-a-service, cloud computing, end-user programming, quantum information processing; and modeling of human-machine systems
- **Capabilities for building evolvable, sustainable, long-lived software-intensive systems:** Exploration of new means to create, keep current, and use engineering artifacts to support long-lived software-intensive systems; new approaches to reliably meet changing requirements and assure security and safety; and long-term retention and archiving of software-development data and institutional knowledge

- **Explore fundamental principles:** Understand, design, analyze, and build software systems that are verifiable, regardless of size, scale, complexity, and heterogeneity, and are correct, assured, efficient, effective, and predictable. Build foundations of software for emerging quantum information science and quantum information processing
- **Develop predictable, timely, cost-effective software-intensive systems**: Disciplined methods, technologies, and tools for systems and software engineering, rapidly evaluating alternative solutions to address evolving needs; measuring, predicting, and controlling software properties and tradeoffs; virtualized and model-based development environments; automation of deterministic engineering tasks; and scalable analysis, test generation, optimization, and verification with traceability to requirements; related issues include:
    - **Software application interoperability and usability**: Develop interface and integration standards, representation methods to enable software interoperability, data exchanges, interoperable databases; supply-chain system integration; and standardized software engineering practices for model development
    - **Cost and productivity issues in development of safety-critical, embedded, and autonomous systems**: Research on composition, reuse, power tools, training, and education to address systems that can be inaccessible after deployment (e.g., spacecraft) and need to operate autonomously
- **Transform SDP frontiers:** Invest in challenging, potentially transformative research; prepare and engage a diverse STEM workforce; sharpen the merit-review process to better identify such research; emphasize interdisciplinary and system-oriented approaches that can lead to transformational concepts
- **Improve health IT interoperability:** Improve conformance testing, testability, and community knowledge of specifications
- **Advance supply chain interoperability for digital manufacturing research**: Use model-based engineering, product manufacturing information standards, and systems engineering standards
- **Assess software quality**: Provide reference datasets and test programs for software assurance and metrics
- **Focus on Smart Grid security guidelines**: Support the multidisciplinary aspects of Smart Grid security

Highlights of the Request

The SDP agencies report the following topical areas as highlights of their planned R&D investments for FY 2016. Agencies are listed in alphabetical order:

- **Software Infrastructure for Sustained Innovation (SI^2)**: Agency-wide program for development and integration of next-generation software infrastructure to advance scientific discovery and education at all levels in the sciences, mathematics, and engineering – NSF
- **Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21)**: Development of new algorithms, tools, and other applications to support innovation – NSF
- **Software and hardware foundations**: Scientific and engineering principles and new logics, languages, architectures, and tools for specifying, designing, programming, analyzing, and verifying software and software-intensive systems; formal methods; V&V tools for sound development of reliable and assured software; formal definitions of weaknesses; standards for certification; and techniques that enable prediction of cost and schedule for large-scale software projects – AFOSR, AFRL, NASA, NIST, NOAA, NSF, ONR, and OSD
- **Computer systems research**: Rethink and transform the software stack for computer systems in different application domains (e.g., new reference architectures for embedded systems); investigate systems that involve computational, human/social, and physical elements – AFOSR, AFRL, NASA, NIST, NSF, ONR, and OSD
- **Intelligent software design**: Investigate approaches to design software-intensive systems that operate in complex, real-time, distributed, and unpredictable environments; invariant refinement of software properties; automation and scaling of testing, validation, and system-level verification; automated analysis of model-based software development; transformational approaches to drastically reduce software life-cycle costs, complexity, and to extend life span; languages and modeling tools that support interoperability, data exchange among engineering tools, large-scale simulations, and federated information systems – AFOSR, NASA, NIST, NOAA, NSF, ONR, and OSD
- **Interoperability standards, knowledge capture processes**: Develop representation schemes for interoperability among computer-aided engineering systems; standards for instrument, mathematical, and measurement data; ontological approaches to facilitate integrating supply-chain systems; interoperability of databases; interoperability testing tools – NIST; and infrastructure for capture, reuse of domain expertise – NOAA, ONR, and OSD
- **Cyber-Enabled Materials, Manufacturing, and Smart Systems (CEMMSS):** Enable smart systems technology framework for advanced manufacturing to establish a scientific basis for engineered systems interdependent with the physical world and social systems; synthesize multidisciplinary knowledge to model and simulate systems in their full complexity and dynamics; this framework expands cyber-physical systems and includes investments in the National Robotics Initiative (NRI), a multiagency activity – NSF
- **Science, Engineering, and Education for Sustainability (SEES):** Explore the role of software in a sustainable energy future to advance science, engineering, and education to inform the societal actions needed for environmental and economic sustainability and sustainable human wellbeing – NSF
- **Quantum Information Sciences**: Support Federal S&T Quantum Information Sciences IWG – NIST

Planning and Coordination Supporting Request

The SDP agencies' current collaboration activities focus on domain areas in which large-scale, software-intensive, and cyber-physical systems predominate – such as in aviation, air-traffic control, and global climate and weather modeling – and on building a forward-looking research agenda to improve the engineering and evolution of such systems. NITRD agencies sponsor workshops to ensure collaboration among the government, industry, and academia (e.g., NSF CPS PI, NSF Secure and Trustworthy Cyberspace [SaTC] PI, and NITRD SDP national needs, opportunities, and priorities workshops).

- **Software verification and validation**: Ongoing collaboration to develop effective approaches for next-generation air transportation – AFRL, FAA, NASA, ONR, and OSD
- **Articulate SDP national needs, opportunities, and priorities:** Provide a focus for the future of software engineering research, and discuss and formulate software and productivity research goals and priorities – SDP agencies
- **Earth System Modeling Framework (ESMF), weather research, and forecasting**: Long-term multiagency efforts to build, use common software toolset, data standards; visualization for weather and climate applications – DoD Service research organizations, DOE/SC, NASA, NOAA, and NSF
- **Automatic program and processor synthesis for data-dependent applications:** From high-level mathematical description, generate code with performance comparable to hand-written code – ONR
- **Automated combinatorial testing of software systems**: Methodology and infrastructure for automated testing that reduces the number of tests – NASA and NIST
- **Next-generation aircraft**: Collaboration on concepts, modeling, and simulation tools – DoD Service research organizations, FAA, NASA, and OSD

Additional 2015 and 2016 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2015 and 2016 under the SDP PCA:

- **AFRL**: Research in new methods, tools for developing reliable, sustainable software-intensive systems for complex real-world environments with human-machine interactions; focus areas include model-based analysis and synthesis, modeling of human-machine interaction, advanced algorithms for real-time and distributed systems, language-based assurance, and formal analysis and verification
- **NASA**: Architecture for SensorWeb for Earth sciences; integrated vehicle health management tools and techniques to enable automated detection, diagnosis, prognosis, and mitigation of adverse events during flight; integrated aircraft control design tools and techniques; and physics-based Multidisciplinary Analysis Optimization (MDAO) framework for cost-effective advanced modeling in development of next-generation aircraft and spacecraft
- **NIST**: Standards development and testing tools supporting interoperability such as schema validation, semantics, automated test generation (conformance testing), naming and design rules; product data models and modeling tools; methods to facilitate 3D shape search; research formal methods for software specification; identify sources of performance variance; develop measurement science that accelerates adoption of roots of trust; develop best practices for managing supply chain risk; identify metrics and methodologies for designed-in security; precisely and accurately define classes of software weaknesses to serve as a basis for tool interoperability and proofs that a tool or technique precludes certain classes of weaknesses; run the Static Analysis Tool Exposition (SATE) to understand the contribution of such tools to assurance; convene Software Testing Metrics and Standards workshop to document state of the art in testing and to map gaps and needed research; tools and metrics to support better quality software and software testing and to support innovation in software-dependent industries
- **NOAA**: Standard and consistent software development practices for environmental modeling; continue adoption of ESMF as part of overall modeling activities; and computer science aspects of software development, including collaboration with universities on programming model for fine-grain parallel architectures
- **NSF**: Advance core research on the science and engineering of software development and evolution, including formal mathematical/logical foundations and automated development methods, programming

languages and methodologies, software testing and analysis, empirical software research, and human-centered computing; coordinate SDP-related areas (e.g., productivity, cost, responsiveness of software, and evolution) in crosscutting topics and programs, including SI^2, SaTC, and effective software design for real-world systems in healthcare, manufacturing, etc.; SEES research on software advances to meet energy requirements in computation and communication; and programmability with assurance underlying key domains such as HPC, health IT, robotics, nanotechnology, and cyber-physical systems

- **ONR**: Automated generation of secure and robust codes from high-level description (design-entry) of functions that lead to software that is both readable and efficient; to methods that automatically capture and use work flow, thought/design-decision documentation during development and sustainment and leads to implementations that meet performance and security requirements; to technologies for real-time control of distributed and embedded systems; to methods for intelligent orchestration of Web services; to language and system for building secure, federated, distributed information systems; to analysis tools for modeling, testing software component interactions; to software for quantum processing; to automated software de-bloating and de-layering to reduce software complexity, size/attack-surface, and achieve highly efficient, compact, secure programs; and to develop novel architectures and protocols for real-time control of embedded sensors, new reference architectures for embedded systems, and promote reusability
- **OSD**: The OSD program addresses composability and timing at all scales, computing for real-time and embedded systems, multicore programming, formal methods, computing at the tactical edge, and software architectures. The OSD program is building on prior initiatives such as the Software Producibility Initiative to mature tools and techniques that improve the efficiency of software production for the DoD. Promising techniques include correct-by-construction methods, model-driven development, validation and verification of complex systems (greater than 20 million lines of code), static and dynamic analysis, deterministic behavior in software, interoperable multiscale and multidomain models, and efficient execution of distributed and multicore processing

Additional Program Focus Areas

Big Data (BD)

Participating Agencies: DARPA, DoD Service Research Organizations, DOE/NNSA, DOE/SC, EPA, NARA, NASA, NIH, NIST, NOAA, NRO, NSA, NSF, OSD, Treasury/OFR, USAID, and USGS

The Big Data Senior Steering Group (BD SSG) was formed in early 2011 to identify current big data research and development activities across the Federal Government; offer opportunities for coordination among agencies, academia, and the private sector; and help establish the goals for a National Big Data R&D Initiative. After a successful multiagency launch in 2012 and an event highlighting multi-stakeholder partnerships in 2013, the focus has turned to synthesizing lessons learned and developing a Federal Big Data Research Agenda that participating agencies can reference when establishing their own big data programs, policies, and activities.

Strategic Priorities

The BD SSG envisions a future in which the ability to analyze and extract knowledge and insights from large, diverse, and disparate data sets will accelerate the progress of scientific discovery and innovation; promote new economic growth; and lead to new fields of research and new areas of inquiry that would otherwise not be possible. The BD SSG has identified four strategic priorities that are consistent across its participating agencies:

- Create next generation capabilities by leveraging emerging big data foundations, technologies, processes, and policies
- Support the R&D necessary to create knowledge from data, but also emphasize the importance of R&D to understand the trustworthiness of data and the resulting knowledge in order to drive breakthrough discoveries that result in confident action
- Build and expand access to the big data resources and cyberinfrastructure – both domain specific and shared – that are needed for agencies to best achieve their mission goals and for the Nation to innovate and benefit
- Improve the national landscape for big data education and training to fulfill increasing demand for both analytical talent and capacity for the broader workforce

Current and Planned Coordination Activities

Building on the shared vision and priorities of its participating agencies, the BD SSG is currently undertaking a series of activities to solicit inputs and ideas to use in the development of a Federal Big Data Research Agenda. Activities include development of an initial big data R&D framework, release of a Request for Information (RFI) to solicit inputs from the general public, and holding a workshop for further discussion and development of inputs. In late 2014, the RFI closed and the submissions were synthesized in preparation for a workshop to be held in January 2015. The workshop will complete the information-gathering phase. The Federal Big Data Research Agenda is expected to be released in fall 2015.

Cyber-Physical Systems (CPS)

Participating Agencies: AFRL, DARPA, DHS, DoD Service Research Organizations, DOE, DOT, FAA, FDA, NASA, NIH, NIST, NSA, NSF, OSD, and USDA/NIFA

The Cyber Physical Systems Senior Steering Group (CPS SSG) was established in 2012 in response to an ongoing effort by NITRD agencies to foster a multidisciplinary research agenda to develop the next-generation of engineered systems—systems that depend on ubiquitous cyber control and require very high levels of system assurance. Establishing the CPS SSG also responded to a PCAST recommendation to NITRD to coordinate a focused research effort on NIT-enabled interaction with the physical world.

Cyber-physical systems are smart networked systems with embedded sensors, processors, and actuators that are designed to sense and interact with the physical world (including human users), and support real-time, guaranteed performance in safety-critical applications. In CPS systems, the joint behavior of the "cyber" and "physical" elements of the system is critical—computing, control, sensing, and networking are deeply integrated into every component, and the actions of components and systems must be carefully orchestrated.

The CPS SSG is exploring the intersection between CPS and robotics in areas where sharing ideas and coordinating efforts could benefit both fields. This past year agencies shared their respective R&D strategies in CPS and robotics. The CPS SSG is now planning a workshop to find common ground for CPS and robotics R&D.

Strategic Priorities

The CPS SSG has developed a vision statement[19] that identifies the following sectors as strategic priorities for research and development. Because CPS technologies are affecting these sectors already, there is the potential for high impact, crosscutting results and for advancing a common body of knowledge in CPS technologies.

- *Agriculture*: Increase efficiency between production and consumption; improve our environmental footprint. Develop high-skill workforce opportunities and sustainable practices, processes, and systems
- *Building controls*: Improve the integration of building infrastructures and the cybersecurity of buildings
- *Defense*: Improve CPS science and technology in complex, networked systems to meet military and national defense needs, especially in engineering resilient systems, cyberspace operations, and autonomous systems
- *Emergency response*: Increase situational awareness and optimize the response of emergency responders through all phases of disaster events such as earthquakes, hurricanes, and man-made disasters
- *Energy*: Develop the smart infrastructure to enable the optimization and management of resources and facilities and allow consumers to control and manage their energy consumption
- *Healthcare*: Design cost-effective, easy-to-certify, and safe products using CPS correct-by-construction design methodologies. Healthcare demands will lead to growth in cyber-physical medical products
- *Manufacturing*: Preserve competitiveness in manufacturing and protect national security. CPS technologies are vital as products' complexity and variety increase while time-to-market decreases
- *Society*: Invest in basic research. "Apps" that network with the physical world are becoming common; consumers want tasks automated and interoperable devices. Commercialization will repay investments
- *Transportation*: Improve efficiency and safety in transportation. Reduce human errors in vehicles and reduce highway congestion; reduce congestion at airports and the rate of runway incursions

[19] Cyber Physical Systems Vision Statement: http://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

The CPS SSG also identified crosscutting strategic challenges that are essential to success in all the sectors:

- *Cybersecurity*: Build resilience to cyber-attacks to ensure safety, wellbeing, and economic stability. Attacks made on the financial system, intelligence databases, and e-commerce sites could be replicated with serious consequences to networked, cyber-physical systems and critical infrastructure such as the Smart Grid, biomedical systems, and transportation networks
- *Economics*: Improve open reference architectures and standards, model-based engineering methodologies, and powerful simulation, verification, and validation tools to reduce the cost of developing CPS systems
- *Interoperability*: Enhance capabilities for assembling individual CPSs into interacting systems of systems
- *Privacy*: Develop mechanisms, policies, and techniques that enable the appropriate use of sensitive and personal information while protecting personal privacy in the context of CPS systems
- *Safety and reliability*: Increase safety and improve reliability of CPS technologies
- *Sociotechnical systems*: Leverage the interactions between people and technology and between complex infrastructures and human behavior to ensure successful cyber-physical system deployments. Approaching such systems from a sociotechnical perspective can ensure that cyber-physical systems satisfy the needs, wants, and aspirations of stakeholders in a positive economic, social, and environmental manner

Current and Planned Coordination Activities

The CPS SSG is pursuing a multiagency, multi-sector, comprehensive focus on crosscutting R&D challenges to address gaps in the Federal CPS R&D portfolio. A concerted effort is necessary to break through the many technical barriers that arise throughout the stages of technology development, from basic science through applied R&D, and that impede the rapid, predictable development and deployment of CPS systems. The approach will be to leverage natural synergies across sectors to learn and advance foundational knowledge. To achieve these goals, the current and planned coordination activities of the CPS SSG include:

- *Coordination Mechanisms*: Provide a variety of mechanisms to enable agency participation in cooperative activities and research funding, including fostering partnerships across industry, academia, and government to address R&D gaps and promote innovation.[20] Highlighted examples of CPS-related coordination on crosscutting R&D include the joint NSF-DHS-DOT Cyber-Physical Systems program solicitation and related Principal Investigator meeting, with additional participation by NASA and other agencies; National Robotics Initiative of NSF, NASA, NIH, and USDA; and Smart and Connected Health program of NSF and NIH. The SSG will continue engaging and collaborating with the High Confidence Software and Systems Coordinating Group (HCSS CG) on R&D activities in CPS and other areas of mutual interest
- *CPS Public Working Group*: Coordinate with the CPS Public Working Group, which is developing consensus definition, taxonomy, and reference architecture for CPS
- *SmartAmerica and Global City Teams Challenges*: Foster innovations and solutions for smart cities; accelerate emerging Internet of Things (IoT) technologies across a range of applications
- *Conferences and Workshops*: Plan and hold a workshop on CPS and Robotics; collaborate and participate with HCSS CG agencies and others in annual conferences with CPS and related focus areas, e.g., CPS Week

[20] Ibid.

Cybersecurity and Information Assurance R&D (CSIA R&D)

Participating Agencies: DHS, NIST, NSA, NSF, ODNI, and OSD

The Cybersecurity and Information Assurance R&D Senior Steering Group (CSIA R&D SSG) was formed in response to the January 2008 Comprehensive National Cybersecurity Initiative (CNCI) – National Security Presidential Directive 54/Homeland Security Presidential Directive 23. This initiative called for the Director of the Office of Science and Technology Policy to "develop a detailed plan to coordinate classified and unclassified cyber research." The purpose of the CSIA R&D SSG is to provide overall leadership for cybersecurity research and development coordination, and to streamline decision processes to support evolving research and budget priorities. The CSIA R&D SSG is composed of senior representatives of agencies with national cybersecurity leadership positions.

Strategic Priorities

The CSIA R&D SSG seeks principally to streamline the communication between research planning among agencies' technical managers and budgetary decision making to accelerate advances in transformative research and deployable technologies. The CSIA R&D SSG is therefore positioned to communicate research needs and proposed budget priorities to policy makers and budget officials. Similarly, the CSIA R&D SSG relays priorities and other pertinent information from higher Federal policy levels to inform R&D coordination activities. The CSIA R&D SSG's strategic priorities include:

- Prioritizing Federal cybersecurity R&D areas and ensuring that the entire spectrum of R&D priorities and key technology challenges across the Federal Government are being addressed
- Leading strategic R&D coordination efforts in addressing Administration priorities
- Formulating and evolving a framework for R&D strategies that focuses on game-changing technologies
- Coordinating R&D objectives and the allocation of Federal budgets to support them

Current and Planned Coordination Activities

The CSIA R&D SSG current and planned activities include:

- Leading, at the request of the OSTP, the development of a National Privacy Research Strategy to serve as a framework to guide Federal R&D investments in privacy-enhancing technologies. This effort is conducted in coordination with other relevant agencies and NITRD SSGs, and aims to develop a strategy that is founded on interagency cooperation and fosters a partnership with commercial, academic, and general public sector stakeholders in addressing the privacy needs of the nation
- Developing and sponsoring events to advance the national research agenda necessary to fulfill key objectives of the Federal cybersecurity R&D strategic plan
- Promoting effective Federal cybersecurity R&D coordination among government agencies and with academia and industry by prioritizing research needs and determining appropriate investment strategies, enabling broad multidisciplinary and multi-sector efforts, enabling agencies to leverage resources, and improving synergy between classified and unclassified Federal research
- Exploring the strategic plan's research themes and how they can drive better security solutions in sectors such as the Smart Grid, health IT, and transportation

Faster Administration of Science and Technology Education and Research (FASTER)

Participating Agencies: AFRL, DOE/SC, DHS, FDIC, IARPA, NARA, NIH, NIST, NOAA, NSF, Treasury, and VA

The Federal Chief Information Officers (CIO) Council, under the leadership of OMB, coordinates the use of IT systems by federal agencies. NITRD, under the leadership of OSTP, coordinates federally supported IT research. The FASTER Community of Practice (CoP) is an association of science agency CIOs and/or their advanced technology specialists, organized under NITRD to improve the communication and coordination between the two interagency entities. The primary focus of FASTER is on the IT challenges specific to supporting the federal scientific research enterprise.

Strategic Priorities

The FASTER CoP has identified several themes to promote the use of advanced IT systems in support of science agency research and development missions. Through coordination and collaboration, FASTER seeks to share information on protocols, standards, best practices, technology assessments, and testbeds, and to accelerate deployment of promising research technology. Consensus among the participants determines the focused theme activities. FASTER serves as a bridge between basic research and operational entities, especially in crosscutting domains. The group's activities are focused on the following strategic themes: cloud computing, cyberinfrastructure, open government (open data and public access), and accelerated communication.

Current and Planned Coordination Activities

FASTER's goal is to enhance collaboration and accelerate agencies' adoption of advanced IT capabilities developed by government-sponsored IT research. FASTER hosts Emerging Technology workshops as well as monthly meetings with invited guest speakers to achieve this goal, including:

- *Cloud computing*: Focuses on issues regarding accessibility and equal access to information for all citizens. Also focuses on procurement issues by concentrating on accepted terminology and metrics for Service Level Agreements (SLAs). FASTER encourages collaboration between NIST and other Federal agencies to progress towards solutions in interoperability, portability, and security for cloud computing activities based on the high-priority requirements identified in the "US Government Cloud Computing Technology Roadmap" (NIST SP 500-293). A workshop held in August 2014 explored avenues to assist cloud customers in the procurement of cloud services by determining methods for constructing high-quality SLAs. The workshop's findings and recommendations centered around the importance of developing requirements for cloud services, standardized language for use in SLAs, and metrics to help in the decision-making process for procuring cloud services
- *Cyberinfrastructure:* Sponsors informal information-sharing exchanges and events with invited guest speakers presenting updates on a variety of national data-focused cyberinfrastructure developments such as data storage, management, integration, analytics, and visualization
- *Open government*: Sponsors informal information-sharing exchanges and events that are responsive to shared interagency interests in Federal digital information sources, open data, and enhancing public access to federally funded research results
- *Accelerated communication*: Promotes timely access to research results, technology assessments, and testbed results for the benefit of the IT operations community and broader audiences. FASTER communications promote the transition of promising technologies from research to practice and allow operational IT challenges and opportunities to be conveyed to the research community in a timely manner

Health Information Technology R&D (HITRD)

Participating Agencies: AHRQ, CDC, DoD, FDA, IHS, NIH, NIST, NSF, ONC, and VA

The Health Information Technology R&D Senior Steering Group (HITRD SSG) was established in the fall of 2010 in response to Section 13202(b) of the American Recovery and Reinvestment Act of 2009 (ARRA, P.L. 111-5), which directed the NITRD Program to include Federal R&D programs related to health IT. In the fall of 2014, the SSG transitioned to a Community of Practice (CoP). HITRD agency participants are working collaboratively to articulate health IT R&D needs for policy and decision makers, and to capitalize on interagency opportunities to advance IT research, innovation, and interoperable health IT systems.

Strategic Priorities

The HITRD CoP coordinates interagency information sharing for health IT R&D planning to promote synergies across Federal health IT investments and to advance IT research for use in healthcare delivery, disease management, disaster and emergency preparedness and response, and lifelong health and wellness. The strategic priorities of the HITRD CoP include:

- Addressing multiagency leadership in health IT interoperability and the development of innovative applications
- Building a health IT research community of information technology and health IT researchers by matching interests to health IT R&D needs
- Enhancing synergies across agencies' complementary health IT research interests

Current and Planned Coordination Activities

The current and planned coordination activities of the HITRD CoP include:

- *Challenges and Prize Competitions*: Exploring ideas, collaborations, and potential engagements to catalyze innovative health IT solutions for the purposes of improving safety and clinical quality, improving adverse event detection and notification, enabling health data use and interoperability, providing decision support aids for maintaining healthy behaviors, and other novel applications of IT for health
- *Research Gaps*: Analyzing IT R&D gaps related to electronic health records (EHRs) and health data access, standards and interoperability, privacy and security, patient-centered outcomes research, evidence-based decision support, modeling and simulation, data analytics, natural language processing, semantic interoperability, knowledge repositories and metadata usage, public health surveillance, patient safety, clinical quality measures, clinical trials, precision medicine, usability, image quality, mobile health and wireless sensors, assistive and medical devices, consumer health IT, and other IT of potential benefit to health and healthcare
- *Health IT R&D Needs*: Assessing health IT R&D needs against the shifting landscape of today's healthcare system that is being transformed, in part, by the widespread adoption of EHRs incentivized by the Meaningful Use program, growth of big data analytics for population health, changes in care payment models, the proliferation of smart apps and mobile health devices for consumers, emerging information technologies, such as wireless health sensors and connectivity through the Internet of Things, and major scientific breakthroughs in understanding molecular processes and the role of the genome in health and disease

Wireless Spectrum R&D (WSRD)

Participating Agencies: DARPA, DHS, DoD Service Research Organizations, DOJ/NIJ, FAA, FCC, NASA, NIST, NSA, NSF, NTIA, and OSD

The Wireless Spectrum R&D Senior Steering Group (WSRD SSG) was established in 2010 in response to the June 28, 2010 *Presidential Memorandum – Unleashing the Wireless Broadband Revolution*.[21] NITRD is supporting the Secretary of Commerce, through NTIA, in consultation with NIST, NSF, DoD, DOJ, NASA, and other agencies, to facilitate research, development, experimentation, and testing by researchers to explore innovative spectrum-sharing technologies.

Strategic Priorities

WSRD SSG member agencies have been funding R&D to enable more efficient use of the radio spectrum through spectrum-sharing technologies. Working within the requirements of the Presidential Memorandum, the WSRD SSG has held a series of workshops to gather information from academic and private sector researchers to help maximize the efforts to increase the use of spectrum sharing in both the government and the private sectors. The WSRD SSG continues to be guided by the following strategic objectives:

- *Transparency*: Communicate to both Federal agencies and the private sector the R&D activities currently being pursued or planned, and help identify areas that still need to be addressed
- *Smart investment*: Develop strategies that can supplement funding for R&D and/or increase the efficiency of existing investments
- *Solicit opportunities*: Identify opportunities for spectrum technology transfer between Federal agencies and the private sector

Current and Planned Coordination Activities

The WSRD SSG has developed a series of reports based on meeting discussions and public-private workshops:

- *Toward Innovative Spectrum Sharing Technologies: A Technical Workshop on Coordinating Federal Government/Private Sector R&D Investment*[22]
- *Federal Government and Private Sector Collaboration on Research Development, Experimentation, and Testing of Innovative Spectrum Sharing Technologies*[23]
- *Research Topics and Proposals to Further the Adoption of Spectrum Sharing*[24]
- *Promoting Economic Efficiency in Spectrum Use: the economic and policy research agenda*[25]
- *Understanding the Spectrum Environment: Data and Monitoring to Improve Spectrum Utilization*[26]

A report on the workshop, "Federal-Commercial Spectrum Data: Understanding Information Exchange Needs, Issues, and Approaches," is in process. A workshop on "Federal – Commercial Spectrum Sharing: Models, Applications and Impacts of Incentives for Sharing" is planned for 2015. The group also maintains two inventories, the *Federal Spectrum Sharing Research Project Inventory*, which is currently being updated and converted into a web portal, and the WSRD Testbed Information Portal.[27]

[21] http://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution, Section 3.
[22] https://www.nitrd.gov/nitrdgroups/images/6/60/WSRD_Workshop_Report_Boulder_July_2011.pdf
[23] https://www.nitrd.gov/nitrdgroups/images/2/20/WSRD_Workshop_II_Report.pdf
[24] https://www.nitrd.gov/nitrdgroups/images/1/15/WSRD_Workshop_III_Report.pdf
[25] https://www.nitrd.gov/nitrdgroups/images/2/2e/WSRD_Workshop_IV_Report.pdf
[26] https://www.nitrd.gov/nitrdgroups/images/8/80/WSRD_Workshop_V_Report.pdf
[27] https://www.nitrd.gov/Subcommittee/wsrd/Testbeds/map.aspx

NITRD Groups and Chairs

Interagency Working Group, Coordinating Group, and Team Chairs

Cyber Security and Information Assurance (CSIA) Interagency Working Group
Co-Chairs
Douglas Maughan, DHS
William D. Newhouse, NIST

High Confidence Software and Systems (HCSS) Coordinating Group
Co-Chairs
David Corman, NSF
William Bradley Martin, NSA
Albert J. Wavering, NIST

High End Computing (HEC) Interagency Working Group
Chair
Lucy Nowell, DOE/SC
Co-Chair
Darren L. Smith, NOAA

Human-Computer Interaction and Information Management (HCI&IM) Coordinating Group
Co-Chairs
Sylvia Spengler, NSF
Vacant

Large Scale Networking (LSN) Coordinating Group
Co-Chairs
Robert J. Bonneau, OSD
Vince Dattoria, DOE/SC
J. Bryan Lyles, NSF

LSN Teams:
Joint Engineering Team (JET)
Co-Chairs
Vince Dattoria, DOE/SC
Kevin Thompson, NSF

Middleware and Grid Interagency Coordination (MAGIC) Team
Co-Chairs
Richard Carlson, DOE/SC
Daniel S. Katz, NSF

Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) Coordinating Group
*Co-Chairs**
C. Suzanne Iacono, NSF
Vacant

SEW Teams:
SEW-Collaboration Team
*Co-Chairs**
Estelle Dodson, NASA
Kara Hall, NCI

SEW-Education Team
*Co-Chairs***
Arlene de Strulle, NSF
William D. Newhouse, NIST (Interim)

Social Computing Team
*Co-Chairs**
Rand Waltzman, DARPA
Vacant

Software Design and Productivity (SDP) Coordinating Group
Co-Chairs
Sol Greenspan, NSF
James Kirby, NRL
Ram D. Sriram, NIST

Video and Image Analytics (VIA) Coordinating Group
Chair
John Garofolo, NIST
Co-Chairs
Richard W. Vorder Bruegge, FBI
Patricia Wolfhope, DHS

Senior Steering Group and Community of Practice Chairs

Big Data (BD) Senior Steering Group
Co-Chairs
Chaitan Baru, NSF
Allen Dearry, NIH
George O. Strawn, NCO

Cyber Physical Systems (CPS) Senior Steering Group
Co-Chairs
Chris L. Greer, NIST
Keith Marzullo, NSF

Cybersecurity and Information Assurance R&D (CSIA R&D) Senior Steering Group
Co-Chairs
Mark A. Luker, NCO
Keith Marzullo, NSF

Faster Administration of Science and Technology Education and Research (FASTER) Community of Practice (CoP)
Co-Chairs
Robert B. Bohn, NIST
Robert Chadduck, NSF

Health Information Technology R&D (HITRD) Community of Practice (CoP)
Co-Chairs
Donald A.B. Lindberg, NIH
George O. Strawn, NCO

Wireless Spectrum R&D (WSRD) Senior Steering Group
Co-Chairs
Mark A. Luker, NCO
Thyagarajan Nandagopal, NSF
Rangam Subramanian, NTIA

*Kevin Crowston, formerly with NSF, was Co-Chair of the SEW CG and SEW-Collaboration and Social Computing Teams through December 2014

**Ernest McDuffie, formerly with NIST, was Co-Chair of the SEW-Education Team through December 2014

Abbreviations and Acronyms

ACS – Advanced Computing Systems
AEH – Airborne electronic hardware
AFOSR – Air Force Office of Scientific Research
AFRL – Air Force Research Laboratory
AHRQ – HHS's Agency for Healthcare Research and Quality
ALCF – Argonne Leadership Computing Facility
ANI – Advanced Networking Initiative
ANL – DOE's Argonne National Laboratory
ARL – Army Research Laboratory
ARO – Army Research Office
ARPA-E – DOE's Advanced Research Projects Agency - Energy
ARSC – Arctic Region Supercomputing Center
ASC – DOE/NNSA's Advanced Simulation and Computing program
ASCR – DOE/SC's Advanced Scientific Computing Research
ASTAM – DHS's Application Security Threat Attack Modeling program
ATC – Air traffic control
ATP – App Testing Portal
BD – Big Data, one of NITRD's Senior Steering Groups
BD2K – NIH's Big Data to Knowledge program
BGPSEC – Border Gateway Protocol Security
BIRN – NIH's Biomedical Informatics Research Network
BISTI – NIH's Biomedical Information Science and Technology Initiative
BlueGene-Q – Latest-generation BlueGene architecture
BLS – U.S. Bureau of Labor Statistics
C3E – ODNI's Computational Cybersecurity in Compromised Environments workshops
C3I – Communications, Command, Control, and Intelligence
CBIIT – NIH's Center for Biomedical Informatics and Information Technology
CCF – Computing and Communication Foundations
CC*DNI – NSF's Campus Cyberinfrastructure – Data, Networking, and Innovation program
CDC – Centers for Disease Control and Prevention
CDS&E – NSF's Computational and Data-Enabled Science and Engineering program
CEDS – DOE/OE's Cybersecurity for Energy Delivery Systems program
CEMMSS – Cyber-enabled Materials, Manufacturing, and Smart Systems
CERDEC – U.S. Army's Communications-Electronics Research, Development, and Engineering Center
CG – Coordinating Group
CGC – DARPA's Cyber Grand Challenge
CIF21 – NSF's Cyberinfrastructure Framework for 21st Century Science and Engineering program
CIO – Chief Information Officer
CISE – NSF's Computer and Information Science and Engineering directorate
CI TraCS – NSF's Fellowships for Transformative Computational Science using CyberInfrastructure
CMATH – DoD/AFRL's Cyber-Based Mission Assurance on Trust-Enhanced Hardware program
CMS – HHS's Centers for Medicare and Medicaid Services
CNCI – Comprehensive National Cybersecurity Initiative
COMPETES – Creating Opportunities to Meaningfully Promote Excellence in Technology, Education, and Science
COOL – DHS's Cybersecurity Organizational/Operational Learning program
CoP – Community of Practice

COTs – Commercial off-the-shelf technologies
CPS – Cyber-physical systems
CRCNS – Collaborative Research in Computational Neuroscience
CSIA – Cybersecurity and Information Assurance, one of NITRD's eight Program Component Areas
DARPA – Defense Advanced Research Projects Agency
DDoS – Distributed Denial of Service
DECIDE – Distributed Environment for Critical Infrastructure Decision-making Exercises
DETER – NSF- and DHS-initiated cyber Defense Technology Experimental Research testbed
DHS – Department of Homeland Security
DIBBs – NSF's Data Infrastructure Building Blocks program, now incorporated into the CC*DNI program
DIMRC – NIH's Disaster Information Management Research Center
DISA – Defense Information Systems Agency
DMZ – Demilitarized Zone; network architecture in which a security layer sits between a trusted, internal network and an untrusted, external network to protect access to the internal network
DNSSEC – Domain Name System Security Extensions
DOC – Department of Commerce
DoD – Department of Defense
DoD (HPCMP) – DoD's High Performance Computing Modernization Program
DoD/MHS – DoD's Military Health System
DoD/TATRC – DoD's Telemedicine and Advanced Technology Research Center
DOE – Department of Energy
DOE/NNSA – DOE's National Nuclear Security Administration
DOE/Oak Ridge – DOE's Oak Ridge National Laboratory
DOE/OE – DOE's Office of Electricity Delivery and Energy Reliability
DOE/SC – DOE's Office of Science
DOJ – Department of Justice
DOT – Department of Transportation
DPIF – Digital Preservation Interoperability Framework International Standard
DREN – DoD's Defense Research and Engineering Network
DTCN – DoD's (ONR) Dynamic Tactical Communications Networks
DTN – Delay-Tolerant Networking
E2E – End-to-End
EARS – Enhancing Access to the Radio Spectrum Program
ECI – Exascale Computing Initiative
ED – Department of Education
EHRs – Electronic health records
ENG – NSF's Engineering directorate
EPA – Environmental Protection Agency
ESG – Earth Systems Grid
ESMF – Earth System Modeling Framework
ESnet – DOE's Energy Sciences Network
ESSC – DOE/SC's Energy Sciences network (ESnet) Steering Committee
FAA – Federal Aviation Administration
FASTER – NITRD's Faster Administration of Science and Technology Education and Research Community of Practice
FBI – Federal Bureau of Investigation
FCC – Federal Communications Commission
FDA – Food and Drug Administration
FHWA – Federal Highway Administration

FIA-NP – NSF's Future Internet Architectures – Next Phase program
FSSCC – Financial Services Sector Coordinating Council
FY – Fiscal Year
Gb – Gigabit
GENI – NSF's Global Environment for Networking Innovations program
GIS – Geographic Information System
GSA – General Services Administration
HACMS – DARPA's High-Assurance Cyber Military Systems
HCI&IM – Human-Computer Interaction and Information Management, one of NITRD's eight Program Component Areas
HCSS – High Confidence Software and Systems, one of NITRD's eight Program Component Areas
HEC – High End Computing
HEC I&A – HEC Infrastructure and Applications, one of NITRD's eight Program Component Areas
HEC R&D – HEC Research and Development, one of NITRD's eight Program Component Areas
HHS – Department of Health and Human Services
HITRD – NITRD's Health Information Technology Research and Development Community of Practice
HPC – High-performance computing
HPCMP – DoD's High Performance Computing Modernization Program
HRD – NOAA's Hurricane Research Division
I/O – Input/output
IARPA – Intelligence Advanced Research Projects Activity
IATS – FHWA'S Integrated Active Transportation System
ICS – Industrial Control Systems
IETF – Internet Engineering Task Force
IHS – Indian Health Services
INCITE – DOE/SC's Innovative and Novel Computational Impact on Theory and Experiment program
InfiniBand – A switched fabric communications link used in high-performance computing and enterprise data centers
Interior – Department of Interior
Internet2 – Higher-education consortium for advanced networking and applications deployment in academic institutions
IPv6 – Internet Protocol, version 6
IRNC – NSF's International Research Network Connections program
ISAP – Multiagency Information Security Automation Program
IT – Information technology
ITS – Institute of Telecommunications Science
ITSEF – Information Technology Security Entrepreneurs' Forum
IWG – Interagency Working Group
JET – LSN's Joint Engineering Team
JETnets – Federal research networks supporting networking researchers and advanced applications development
K-12 – Kindergarten through 12th grade
LANL – DOE's Los Alamos National Laboratory
LBNL – DOE's Lawrence Berkeley National Laboratory
LCF – DOE's Leadership Computing Facility
LLNL – DOE's Lawrence-Livermore National Laboratory
LSN – Large Scale Networking, one of NITRD's eight Program Component Areas
LTE – Long Term Evolution, a standard for wireless data communications technology
MAGIC – LSN's Middleware and Grid Interagency Coordination Team

MIC – Many integrated cores
MDAO – Multidisciplinary analysis optimization
MOU – Memorandum of Understanding
MURI – Multidisciplinary University Research Initiative
NARA – National Archives and Records Administration
NAS – NASA Advanced Supercomputing facility
NASA – National Aeronautics and Space Administration
NCAR – NSF-supported National Center for Atmospheric Research
NCBC – NIH's National Centers for Biomedical Computing
NCCoE – National Cybersecurity Center of Excellence
NCCS – NASA Center for Climate Simulation
NCI – NIH's National Cancer Institute
NCO – NITRD's National Coordination Office
NCR – National Cyber Range program
NERC-CIP – North American Electric Reliability Corporation's Critical Infrastructure Protection
NERSC – DOE/SC's National Energy Research Scientific Computing Center
NeTS – NSF's Networking Technology and Systems program
NextGen – Next Generation Air Transportation System
NEX – NASA Earth Exchange
NICE – National Initiative for Cybersecurity Education
NIGMS – NIH's National Institute of General Medical Sciences
NIH – National Institutes of Health
NIJ – DOJ's National Institute of Justice
NIST – National Institute of Standards and Technology
NITRD – Networking and Information Technology Research and Development
NLM – NIH's National Library of Medicine
NOAA – National Oceanic and Atmospheric Administration
NRC – Nuclear Regulatory Commission
NREIP – Naval Research Enterprise Summer Intern Program
NRI – National Robotics Initiative
NRL – Naval Research Laboratory
NSA – National Security Agency
NSF – National Science Foundation
NSF/MPS – NSF's Directorate for Mathematical and Physical Sciences
NSF/SBE – NSF's Directorate for Social, Behavioral, and Economic Sciences
NSTC – National Science and Technology Council
NSTIC – National Strategy for Trusted Identities in Cyberspace
NTIA – National Telecommunications and Information Administration
NTSB – National Transportation Safety Board
NTP – Network Time Protocol
N-Wave – NOAA's high speed network
ODNI – Office of the Director of National Intelligence
OFR – Treasury's Office of Financial Research
OLCF – Oak Ridge Leadership Computing Facility
OMB – White House Office of Management and Budget
ONC – HHS's Office of the National Coordinator for Health Information Technology
ONR – Office of Naval Research
OpenFlow – Open protocol for software-defined networks
OOMMF – Object-Oriented Micromagnetics Modeling Framework

ORCA – Online Representations and Certifications Application
ORNL – DOE's Oak Ridge National Laboratory
OS – Operating system
OSD – Office of the Secretary of Defense
OSG – Open Science Grid
OSTP – White House Office of Science and Technology Policy
PCA – Program Component Area
PCAST – President's Council of Advisors on Science and Technology
perfSONAR – performance Services-Oriented Network Architecture
PF – Petaflop(s), a thousand teraflops
PI – Principal investigator
PREDICT – DHS's Protected Repository for the Defense of Infrastructure Against Cyber Threats
PROCEED – AFRL and DARPA's PROgramming Computation on EncryptEd Data program
QOS – Quality of Service
R&D – Research and development
RDA – Research Data Alliance
RDT&E – DoD's Research Development Test & Evaluation programs
ROV – Remotely operated vehicle
RSIG – Remote Sensing Information Gateway
S&T – Science and technology
S4C – Science for Cybersecurity
S5 – Safe and Secure Software and Systems Symposium
SaTC – NSF's Secure and Trustworthy Cyberspace program
SAMATE – Software Assurance Metrics and Tool Evaluation
SATCOM – Satellite communications
SATE – NIST's Static Analysis Tool Exposition
SBIR – Small Business Innovation Research, a Federal grant program
SCADA – Supervisory control and data acquisition
SCAP – Security Content Automation Protocol
SciDAC – DOE/SC's Scientific Discovery through Advanced Computing program
SDN – Software Defined Network
SDP – Software Design and Productivity, one of NITRD's eight Program Component Areas
SDSC – San Diego Supercomputer Center
SEI – Software Engineering Institute
SEES – NSF's Science, Engineering, and Education for Sustainability program
SensorWeb – NASA infrastructure of linked ground and space-based instruments to enable autonomous collaborative observation
SEW – Social, Economic, and Workforce Implications of IT and IT Workforce Development, one of NITRD's eight Program Component Areas
SEW-Ed – SEW's Education Team
SGIP – Smart Grid Interoperability Panel
SI^2 – NSF's Software Infrastructure for Sustained Innovation program
SME – Subject Matter Expert
SNL – Sandia National Laboratories
SSG – Senior Steering Group
STAMP – DHS's Static Tool Analysis Modernization Project
STARSS – Secure, Trustworthy, Assured and Resilient Semiconductors and Systems
State – Department of State
STEM – Science, technology, engineering, and mathematics

STONESOUP – IARPA's Security Taking on New Executable Software of Uncertain Provenance activity
SWAMP – DHS's Software Assurance Marketplace
SWAP – Size, Weight, And Power
TACC – Texas Advanced Computing Center
TAS – Technology Auditing Service
TCIPG – DHS- and DOE-supported Trustworthy Cyber Infrastructure Protection for the Power Grid program, with initial funding also from NSF
TeraGrid – NSF terascale computing grid, now succeeded by eXtreme Digital (XD) program
TF – Teraflop(s), a trillion floating-point operations per second
TIC – Trusted Internet Connection
TIES – DoD's Tactical Infrastructure Enterprise Services
TIS – NSF's XD Technology Insertion Service program
Treasury – Department of the Treasury
UAS – Unmanned Aircraft Systems
UAV – Unmanned aerial vehicle
UQ – Uncertainty quantification
USAF – United States Air Force
USAID – United States Agency for International Development
USDA – U.S. Department of Agriculture
USGCB – U.S. Government Configuration Baseline
USGS – U.S. Geological Survey
USHIK – United States Health Information Knowledgebase
V&V – Verification and Validation
VA – Department of Veterans Affairs
VOSS – NSF's Virtual Organizations as Sociotechnical Systems program
VSTTE – Verified software, theories, tools, and experiments
VTC – Video Teleconferencing
VVUQ – Verification and Validation, Uncertainty Quantification
WAIL – NSF's Wisconsin Advanced Internet Laboratory
WAN – Wide area network
WSRD – Wireless Spectrum Research and Development, one of NITRD's Senior Steering Groups
XD – NSF's eXtreme Digital program
XPS – NSF's eXploiting Parallelism and Scalability program
XSEDE – NSF's Extreme Science and Engineering Discovery Environment

NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

SUBCOMMITTEE ON NETWORKING AND
INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT

Suite II – 405, 4201 Wilson Blvd., Arlington, VA 22230

703-292-4873

www.nitrd.gov