THE NETWORKING AND INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT PROGRAM

SUPPLEMENT TO THE PRESIDENT'S BUDGET

FY 2014

MAY 2013

Networking and Information Technology Research and Development
National Coordination Office

George O. Strawn
Director

Mark A. Luker
Associate Director

Margaret E. Harmsen
Editor, FY 2014 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 2014 Budget Request. It describes the activities underway in 2013 and planned for 2014 by the federal agencies participating in the NITRD Program, primarily from a programmatic and budgetary perspective. It reports actual investments for FY 2012and requested investments for FY 2014 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 2013 and 2014 activities by agency.

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

SUPPLEMENT TO THE PRESIDENT'S BUDGET

FOR FISCAL YEAR 2014

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

MAY 2013

National Science and Technology Council Committee on Technology

Thomas C. Power, Chair, OSTP
Pedro Espina, Executive Secretary, OSTP

Subcommittee on Networking and Information Technology Research and Development

Co-Chairs
Farnam Jahanian, NSF
George O. Strawn, NCO

Department of Commerce

NIST
Representative
Charles H. Romine
Alternate
Kamie Roberts

NOAA
Representative
David Michaud
Alternate
Darren L. Smith

Department of Defense

DARPA
Representative
Daniel Kaufman

NSA
Representative
Deborah A. Frincke
Alternate
Candace S. Culhane

OSD
Representative
Robert Gold
Alternate
Dai H. Kim

SERVICE RESEARCH ORGANIZATIONS:

Air Force
Representative
Russell Partch

Army
Representative
Mary J. Miller
Alternate
Kristopher E. Gardner, Sr.

Navy
Representative
Sukarno Mertoguno

Department of Energy

DOE/NNSA
Representative
Robert Meisner
Alternate
Thuc T. Hoang

DOE/OE
Representative
Carol Hawk

DOE/SC
Representative
Barbara Helland
Alternate
William Harrod

Department of Health and Human Services

AHRQ
Representative
J. Michael Fitzmaurice
Alternate
P. Jon White

NIH
Representative
Amy L. Swain
Alternate
Peter M. Lyster

ONC
Representative
Douglas B. Fridsma

Independent Agencies

DHS
Representative
Douglas Maughan
Alternate
Luke Berndt

EPA
Representative
Gary L. Walter

NASA
Representative
Bryan A. Biegel
Alternate
James R. Fischer

NARA
Representative
Michael Wash

NRO
Representative
Robert Jimenez
Alternate
Richard D. Ridgley

NSF
Representatives
Farnam Jahanian
Alan Blatecky
Alternate
C. Suzanne Iacono

OMB
Representative
Arti Garg

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

May 10, 2013

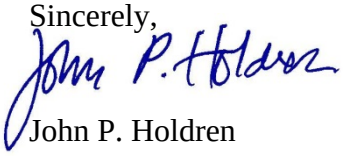
Dear Members of Congress:

I am pleased to transmit with this letter the FY 2014 annual report of the Federal Government's multiagency Networking and Information Technology Research and Development (NITRD) program. The NITRD program, which today comprises 20 member agencies and benefits from the contributions of many other agencies, coordinates Federal research and development investments in the advanced digital technologies that are so essential for the Nation's economic growth and prosperity in the 21st century.

In less than a generation, networking and computing technologies have transformed the lives of all Americans and have catalyzed enormous changes in business, government, and education. Advances in cutting-edge digital technologies have been pivotal to U.S. economic growth, innovation, and job creation, and will be essential to the generation of new capabilities in the sciences, education, telecommunications, and national security, among other domains. As the President has made clear, such networking and computing capabilities will also provide critical foundations for a number of specific policy priorities, including an improved health care system; increased development of sustainable energy sources and energy delivery systems; and a more resilient and secure Internet.

The Federal NITRD investments we make 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

Executive Summary

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. The multiagency NITRD Program seeks to:

- Provide research and development foundations for assuring continued U.S. technological leadership in advanced networking, computing systems, software, and associated information technologies
- Provide research and development foundations for meeting the needs of the Federal Government for advanced networking, computing systems, software, and associated information technologies
- Accelerate development and deployment of these technologies in order to maintain world leadership in science and engineering; enhance national defense and national and homeland security; improve U.S. productivity and competitiveness and promote long-term economic growth; improve the health of the U.S. citizenry; protect the environment; improve education, training, and lifelong learning; and improve the quality of life

Over the last 12 months the NITRD Program welcomed the Department of Energy's Office of Electricity Delivery and Energy Reliability (DOE/OE) and the National Reconnaissance Office (NRO) as new members. The program also established the Cyber Physical Systems Senior Steering Group (CPS SSG) to coordinate a new program focus area in cyber-physical systems.

In the past year, the NSTC released the *NITRD Program 2012 Strategic Plan*.[1] The five-year Strategic Plan presents NITRD's overarching vision for the digital world in the 21st century – a world in which high speed networks, systems, software, devices, data, and applications are fully secure, safe, reliable, multimodal, and easy to use. The Strategic Plan outlines three essential foundations for advancing leadership in the digital world:

- *WeCompute* – Expanded human-computer partnerships, including more capable, available, and affordable systems; more powerful digital tools for people; and new forms of collaboration between the two
- *Trust and Confidence* – The ability to design and build systems with levels of security, safety, privacy, reliability, predictability, and dependability that "you can bet your life on"
- *Cyber Capable* – Transformed education and training to ensure that current generations benefit fully from cyber capabilities and to inspire a diverse, prepared, and highly productive next-generation workforce of cyber innovators.

The NITRD Strategic Plan responds to the August 2007 assessment of the NITRD Program by the President's Council of Advisors on Science and Technology (PCAST). In January 2013 the PCAST released the report, *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*,[2] which offers the PCAST's latest assessment of the NITRD Program. A review of the assessment and response to the PCAST's recommendations are currently underway.

The FY 2014 budget guidance on science and technology priorities from the OMB and OSTP underscored the critical importance of IT R&D to the Nation by highlighting multiagency research in information technology R&D as a priority and specifically prioritizing investments in big data and cybersecurity R&D. The budget requests by NITRD member agencies in this FY 2014 Supplement align well with the OMB-OSTP guidance.

[1] *NITRD Program 2012 Strategic Plan.* http://www.nitrd.gov/pubs/strategic_plans/2012_NITRD_Strategic_Plan.pdf
[2] *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*. Report to the President and Congress. http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf

NITRD Member Agencies

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

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

Department of Defense (DoD)
- Defense Information Systems Agency (DISA)
- Intelligence Advanced Research Projects Activity (IARPA)
- Military Health System (MHS)
- Telemedicine and Advanced Technology Research Center (TATRC)

Department of Education (ED)
Department of Energy (DOE)
- Advanced Research Projects Agency-Energy (ARPA-E)

Department of Health and Human Services (HHS)
- Centers for Disease Control and Prevention (CDC)
- Centers for Medicare and Medicaid Services (CMS)
- Food and Drug Administration (FDA)
- Indian Health Service (IHS)
- Office of the Assistant Secretary for Preparedness and Response (ASPR)

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

Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)

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)
General Services Administration (GSA)
Joint Planning and Development Office (JPDO)
National Transportation Safety Board (NTSB)
Nuclear Regulatory Commission (NRC)
Office of the Director of National Intelligence (ODNI)
U.S. Agency for International Development (USAID)
U.S. Department of Agriculture (USDA)

The NITRD Program

About the NITRD Program

Now in its 22nd year, NITRD is one of the oldest and largest of the formal federal programs that engage multiple agencies. 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), NITRD provides a framework and mechanisms for coordination among the federal agencies that support advanced IT R&D and report IT research budgets in the NITRD crosscut. Many other agencies with IT interests also participate informally in NITRD activities.

Agencies coordinate their NITRD research activities and plans in Program Component Areas (PCAs). The PCAs are identified as an Interagency Working Group (IWG) or a Coordinating Group (CG) and report their R&D budgets as a crosscut of the NITRD agencies. They are charged with facilitating interagency program planning, developing and periodically updating interagency roadmaps, developing recommendations for establishing federal policies and priorities, summarizing annual activities for the NITRD Program's Supplement to the President's Budget, and identifying potential opportunities for collaboration that have been identified by the Office of Management and Budget (OMB) and the Office of Science and Technology Policy (OSTP) as priorities for federal coordination and collaboration. 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)

In each of these R&D areas, agency program managers meet in an IWG or CG to exchange information and collaborate on research plans and activities such as implementing 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, information technology (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.

Since 2008, the NITRD Program has given focus to emerging science and technology priorities by forming interagency Senior Steering Groups (SSGs) to work collaboratively on developing effective R&D strategies for national-level IT challenges. Implementing such R&D strategies may require multidisciplinary, multiagency, and multi-sector efforts and modifications to existing federal R&D programs and policies. Thus, SSGs offer a means of cross-agency collaboration for senior-level individuals who have the authority to affect or shape the R&D directions of their organizations. The program focus areas coordinated by SSGs include:

- Big Data Research and Development (BD)
- Cyber Physical Systems Research and Development (CPS) – *new in 2012*
- Cybersecurity and Information Assurance Research and Development (CSIA R&D)
- Health Information Technology Research and Development (HITR&D)
- Wireless Spectrum Research and Development (WSR&D)

Additionally, the NITRD Program coordinates a group of science agency Chief Information Officers (CIOs) and/or their advanced technology specialists in a Community of Practice (CoP) with the goal of enhancing collaboration and accelerating agencies' adoption of advanced IT capabilities developed by government-sponsored IT research. The CoP is:

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

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, CoP, and SSGs 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: http://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:

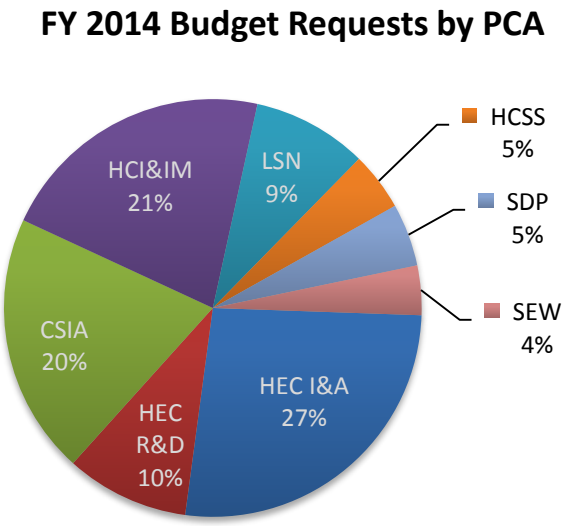
- Listing of the NITRD member agencies and participating agencies active in the PCA
- Definition of the research covered in the PCA
- Strategic priorities in the PCA for the forthcoming fiscal year
- Budget highlights – agencies' key R&D programs and topical emphases in the PCA for the forthcoming year
- 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.

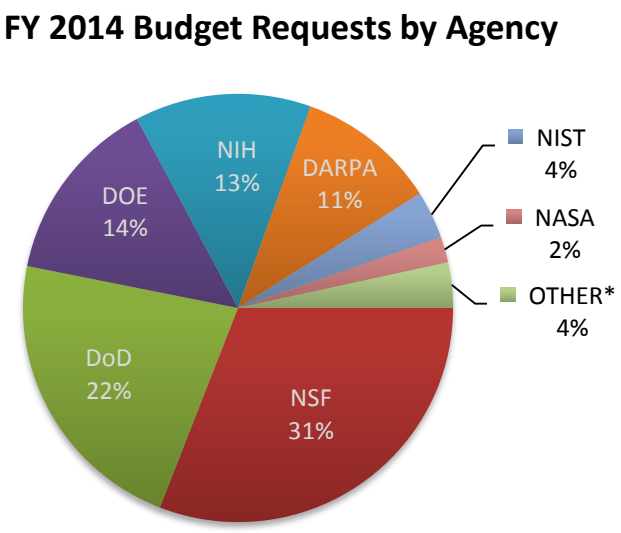
In addition, the NITRD Supplement provides brief summaries of the interagency program focus areas coordinated under the NITRD Program's CoP and SSGs, including each group's strategic priorities and current and planned coordination activities for the forthcoming year.

The President's FY 2014 budget request for the NITRD Program is $3.968 billion and the 2012 NITRD actual expenditures totaled $3.810 billion. Details of the budget are presented in the table on pages 8-9 and discussed in the budget analysis section.

The following illustration shows the percentages of the FY 2014 budget requests by PCA.

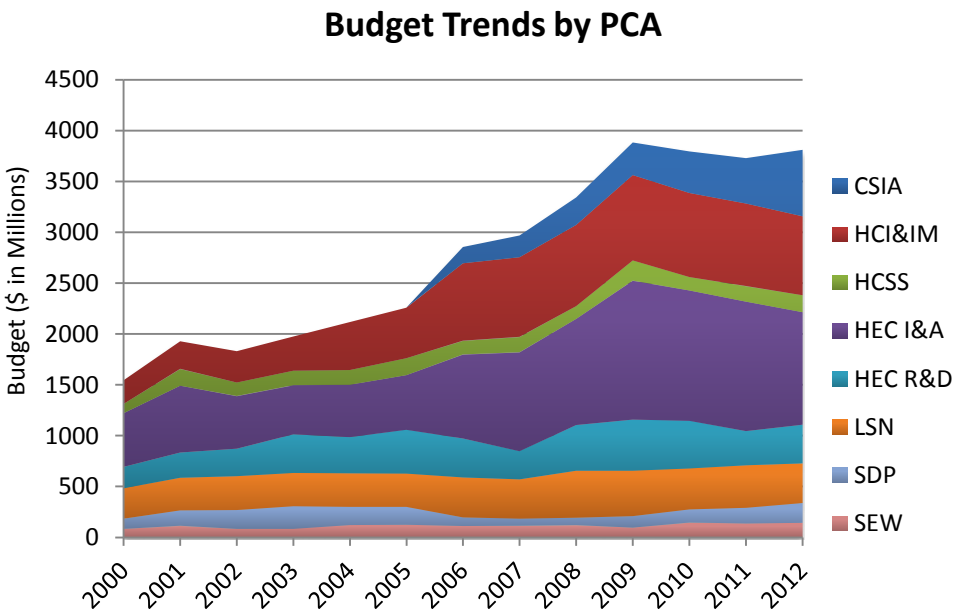


The following illustration shows the percentages of the FY 2014 budget requests by agency.

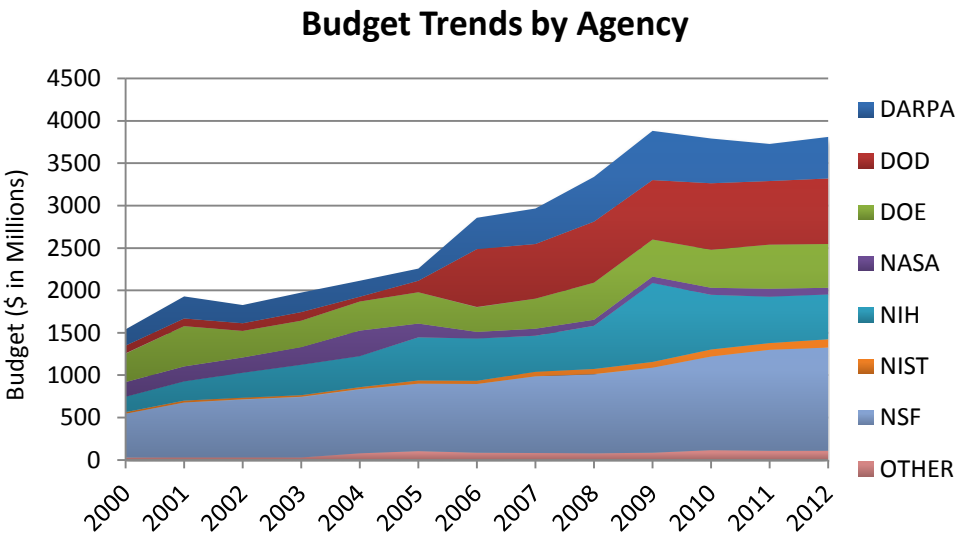


*Includes AHRQ, DHS, EPA, NARA, and NOAA.

The following illustration shows budget trends by PCA since FY 2000.[3]



The following illustration shows budget trends by agency since FY 2000.[4]



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

[3] The budget trends illustrations use budget estimates for FY 2000 - FY 2009 and budget actuals for FY 2010 and beyond.
[4] Same as footnote 3.

This page intentionally left blank.

Agency NITRD Budgets by Program Component Area

Key: FY 2012 Budget Actuals, *FY 2013 Levels*, and **FY 2014 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[5]
	FY 2012 Actual	99.2	88.4	329.3	109.6	270.6	127.6	106.5	85.2	1,216.3
	FY 2013 Level[6]	—	—	—	—	—	—	—	—	—
NSF	**FY 2014 Request**	**114.3**	**103.3**	**248.4**	**113.6**	**299.9**	**136.3**	**122.0**	**89.6**	**1,227.4**
		203.8	38.3	178.9	64.9	122.7	141.3		22.4	772.3
		—	—	—	—	—	—		—	—
DoD[7]		**242.9**	**32.1**	**198.7**	**51.1**	**218.6**	**122.4**		**15.7**	**881.5**
		33.5	0.8	314.3	93.1		49.9	6.0		497.7
		—	—	—	—	—	—	—	—	—
DOE[8]		**41.5**	**1.1**	**327.1**	**108.1**		**63.4**			**541.2**
			10.8	198.7	27.8	193.4	8.0	22.0	71.4	532.2
			—	—	—	—	—	—	—	—
NIH			**10.9**	**190.8**	**28.2**	**194.7**	**8.1**	**22.2**	**72.0**	**526.7**
		223.0			75.0	138.0	53.0			489.0
		—			—	—	—			—
DARPA		**265.8**			**66.7**	**78.6**	**7.5**			**418.6**
		45.0	8.7	15.3	5.6	11.4	6.7		4.3	97.1
		—	—	—	—	—	—		—	—
NIST		**68.0**	**14.2**	**16.5**	**5.6**	**22.2**	**10.8**	**1.0**	**5.3**	**143.7**
		49.4						5.0		54.4
		—						—		—
DHS		**70.5**				**2.2**		**3.8**		**76.5**
			18.0	39.2	0.3	10.3	0.8		9.4	77.9
			—	—	—	—	—		—	—
NASA			**16.5**	**39.2**	**0.6**	**9.5**	**1.0**		**9.6**	**76.4**
				19.4			1.9		0.7	22.0
				—			—		—	—
NOAA				**21.4**	**0.2**	**0.5**	**3.3**		**0.7**	**26.1**
						25.1	0.5			25.6
						—	—			—
AHRQ						**25.1**	**0.5**			**25.6**
				9.0	5.0			4.0		18.0
				—	—			—		—
DOE/NNSA[9]				**9.0**	**5.0**			**3.0**		**17.0**

[5] Totals may not sum correctly due to rounding.
[6] FY 2013 levels are left blank (shown as a "—") pending finalization of FY 2013 funding levels.
[7] DoD budget includes funding from OSD, NRO, NSA, 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) and High Performance Computing Modernization Program (HPCMP) are under Army. Although DARPA, NSA, and OSD research organizations are under DoD, they are independent of the research organizations of the DoD Services (Air Force, Army, and Navy).
[8] DOE budget includes funding from DOE's Offices of Science (SC), Electricity Delivery and Energy Reliability (OE), Energy Efficiency and Renewable Energy (EERE), and Advanced Research Projects Agency - Energy (ARPA-E).
[9] DOE/NNSA includes only funds spent on engagements with industry. It does not include significant funding for engineering, procurement, and integration funding in the Advanced Supercomputing Campaign.

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[5]
	FY 2012 Actual			3.0		3.0				6.0
	FY 2013 Level[6]			—		—				—
EPA	**FY 2014 Request**			**3.0**		**3.0**				**6.0**
DOT[10]			**1.5**							**1.5**
						1.0				1.0
						—				—
NARA						**0.2**				**0.2**
Total FY 2012 Actuals[5]		653.9	165.0	1,107.0	381.3	775.6	389.7	143.5	193.4	3,809.5
Total FY 2013 Levels[6]		—	—	—	—	—	—	—	—	—
Total FY 2014 Requests[5]		**803.0**	**179.6**	**1,054.1**	**379.0**	**854.5**	**353.4**	**152.0**	**192.8**	**3,968.4**

NITRD Program Budget Analysis

Fiscal Year Overview for 2012-2014

In the following analysis of the NITRD Program, the President's FY 2014 request is compared with FY 2012 actual spending. 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. In addition, the NITRD agencies have continued to work collectively on improving the PCA definitions, as reflected by changes in the definitions outlined in OMB Circular A-11, and individually on improving the classification of investments within the PCAs, resulting in changes in NITRD Program budgets.

Summary

The President's 2014 budget request for the NITRD Program is $3.968 billion, an increase of $0.158 billion, approximately 4.15 percent, more than the $3.810 billion 2012 actual expenditures. 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 2012 actual spending and 2014 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.

DARPA

Comparison of 2012 actual ($489.0 million) and 2014 request ($418.6 million): The $70.4 million decrease is primarily due to decreases of $59.4 million in HCI&IM following completion of Machine Reading and Reasoning Technology efforts and $45.5 million in LSN for drawdown of the Transformative Apps and Wireless Networking efforts prior to transition, with smaller decreases in other PCAs, partially offset by an increase of $42.8 million in CSIA for the expansion of DARPA's Foundational Cyber Warfare (Plan X) program that is developing technologies for comprehensive awareness and understanding of the cyber battlespace.

DHS

Comparison of 2012 actual ($54.4 million) and 2014 request ($76.5 million): The $22.1 million increase results primarily from an increase of $21.1 million in CSIA for R&D in cyber economic incentives, tailored trustworthy

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

spaces, moving target defense, transition to practice, and software assurance, with smaller increases and decreases in other PCAs.

DoD

Comparison of 2012 actual ($772.3 million) and 2014 request ($881.5 million): The $109.2 million increase is primarily due to increases of $39.1 million in CSIA, $19.8 million in HEC I&A, $95.9 in HCI&IM, partially offset by decreases of $13.8 million in HEC R&D and $18.9 million in LSN, with smaller decreases in other PCAs.

DOE

Comparison of 2012 actual ($497.7 million) and 2014 request ($541.2 million): The $43.5 million increase is primarily due to increases of $12.8 million in HEC I&A, which supports research focused on the linked challenges of exascale hardware (such as energy management and fault tolerance) and on data-intensive science; $15.0 million in HEC R&D, which supports the second phase of FastForward to develop critical technologies for exascale computing; $13.5 million in LSN to support the rollout of 100 Gbps network capabilities to the National laboratories and other DOE sites; and smaller increases and decreases in other PCAs.

NIST

Comparison of 2012 actual ($97.1 million) and 2014 request ($143.7 million): The increase of $46.6 million includes $23.0 million in CSIA for new initiatives in cybersecurity R&D, cybersecurity standards, and grants for the National Strategy for Trusted Identities in Cyberspace (NSTIC); $10.8 million in HCI&IM for new initiatives in cyber-physical systems, health IT, and advanced materials; and smaller increases in other PCAs for new initiatives in advanced communications, advanced materials, cyber-physical systems, health IT, the National Initiative for Cybersecurity Education (NICE), and smart manufacturing.

NSF

Comparison of 2012 actual ($1,216.3 million) and 2014 request ($1,227.4 million): The increase of $11.1 million is primarily due to increases of $15.1 million in CSIA for the Secure and Trustworthy Cyberspace (SaTC) program; $14.9 million in HCSS for increased investments in the National Robotics Initiative (NRI) and in cyber-physical systems as part of the Cyber-Enabled Materials, Manufacturing, and Smart Systems (CEMMSS) investment; $29.3 million in HCI&IM for increased investments in NRI as well as Cyberinfrastructure Framework for 21st Century Science and Engineering (CIF21) investments in big data; $15.5 million in SEW for the NRI to focus on human-centered research in developing service robots, support for big data and e-science collaboration tools as part of CIF21, and support for cyberlearning and on-line education programs; and smaller increases in other PCAs, partially offset by a decrease of $80.9 million in HEC I&A. The HEC I&A FY 2012 actual includes obligations of $71.6 million over the enacted level for NSF due to recoveries of prior year unpaid obligations that were re-obligated in FY 2012.

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 2012 actual spending and 2014 requests. The changes are described below.

CSIA

Comparison of 2012 actual ($653.9 million) and 2014 request ($803.0 million): The $149.1 million increase is largely due to increases of $15.1 million at NSF, $39.1 million at DoD, $42.8 million at DARPA, $23.0 million at NIST, $21.1 at DHS, and smaller increases at other agencies.

HCI&IM

Comparison of 2012 actual ($775.6 million) and 2014 request ($854.5 million): The $78.9 million increase is largely due to increases of $29.3 million at NSF, $95.9 million at DoD, and $10.8 million at NIST, with smaller increases and decreases at other agencies, partially offset by a decrease of $59.4 million at DARPA.

HCSS

Comparison of 2012 actual ($165.0 million) and 2014 request ($179.6 million): The $14.6 million increase is largely due to an increase of $14.9 million at NSF, with smaller increases and decreases at other agencies.

HEC I&A

Comparison of 2012 actual ($1,107.0 million) and 2014 request ($1,054.1 million): The $52.9 million decrease is largely due to a decrease of $80.9 million at NSF, with smaller increases and decreases at other agencies, partially offset by increases of $19.8 million at DoD and $12.8 at DOE.

LSN

Comparison of 2012 actual ($389.7 million) and 2014 request ($353.4 million): The $36.3 million decrease is largely due to decreases of $18.9 million at DoD and $45.5 million at DARPA, with smaller increases and decreases at other agencies, partially offset by an increase of $13.5 million at DOE.

Budget Request by Program Component Area

Cyber Security and Information Assurance (CSIA)

NITRD Agencies: AFOSR, AFRL, ARL, ARO, CERDEC, DARPA, DHS, 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 concern 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; and reconstitution of computer-based systems and data.

President's FY 2014 Request

Strategic Priorities Underlying This Request

In December 2011, the White House Office of Science and Technology Policy released *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*—a framework for a set of coordinated federal strategic priorities and objectives for cybersecurity research. The Strategic Plan continues to define federal research priorities in cybersecurity into FY 2014. The Plan defines four areas for prioritizing research and development activities:

- **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 Moving Target, Tailored Trustworthy Spaces, Designed-In Security, and Cyber Economic Incentives
- **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 IT and Smart Grid
- **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

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 2014. 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.
    - Trusted foundation for defensive cyberspace operations – AFRL, ARL, ARO, CERDEC, ONR, and OSD

- High assurance security architectures – AFRL, DARPA, NIST, NSA, ONR, and OSD
- Tactical Assured Information Sharing Project – OSD
- IT Security Automation/Continuous Monitoring/Security Content Automation Protocol Program – DHS, NIST, and NSA
- Security for cloud-based systems – AFOSR, AFRL, DARPA, DHS, and NIST
- Secure wireless networking – ARL, ARO, CERDEC, DARPA, NSA, ONR, and OSD
- Secure and Trustworthy Cyberspace (SaTC) Program – NSF
- Digital Provenance and Hardware-Enabled Trust Programs – DHS
- Content and Context Aware Trusted Router (C2TR) – AFRL
- Bio-Inspired Technologies for Enhancing Energy Sector Cybersecurity – DOE/OE
- Cross-layer resilient and adaptive networking – OSD/NRL
- Cyber Agility Program – AFRL

- **Moving Target theme**: Develop capabilities to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and the cost for attackers, limit the exposure of vulnerabilities and malicious opportunities, and increase system resiliency.
  - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
  - Cyber Unification of Security Hardening and Protection of Operational Frameworks (CRUSHPROOF) – ARL, ARO, CERDEC, and OSD
  - Morphing Network Assets to Restrict Adversarial Reconnaissance (Morphinator) – ARL, ARO, and CERDEC
  - Defensive Enhancements for Information Assurance Technologies (DEFIANT) – ARL, ARO, and CERDEC
  - Moving Target Defense Program – DHS
  - Proactive and Reactive Adaptive Systems – NSA
  - Security Automation and Vulnerability Management – NIST
  - Trust Management in Service Oriented Architectures – ONR
  - Robust Autonomic Computing System – ONR
  - Information Security Automation Program (ISAP) – DHS, NIST, and NSA
  - Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) and Mission-Oriented Resilient Clouds (MRC) Programs – DARPA
  - Network Randomization for the Energy Sector – DOE/OE
- **Cyber Economic Incentives theme**: Develop effective market-based, legal, regulatory, or institutional incentives to make cybersecurity ubiquitous, including incentives affecting individuals and organizations.
  - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
  - Cyber Economics Incentives Research Program – DHS
  - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) – DOE/OE

- **Designed-in Security theme**: Develop capabilities to design and evolve high-assurance, software-intensive systems predictably and reliably while effectively 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.
  - Survivable Systems Engineering – OSD
  - Trusted Computing – AFRL, NSA, and OSD
  - Software Development Environment for Secure System Software and Applications – ONR
  - Roots of Trust – AFRL, NIST, and NSA
  - Software Assurance Metrics And Tool Evaluation (SAMATE) – DHS and NIST
  - Automated Program Analysis for Cybersecurity (APAC) – DARPA
  - High-Assurance Cyber Military Systems (HACMS) – DARPA
  - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
  - Cybersecurity for Energy Delivery Systems (CEDS) Program – DOE/OE

- **Developing Scientific Foundations**
  - **Science of Security**: In anticipation of the challenges in securing the cyber systems of the future, the 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.
    - Science for Cybersecurity (S4C) – ARL and ARO
    - Science of Security MURI – AFOSR
    - Trust and Suspicion Basic Research Initiative – AFOSR
    - Cyber Measurement Campaign (CMC) – OSD
    - Cyber-Physical Survivability Metrics – DOE/OE
  - **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

- **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.
    - Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) – DHS and DOE/OE
    - National Strategy for Trusted Identities in Cyberspace (NSTIC) – NIST
    - Health IT Security Program – NIST

- Smart Grid Interoperability Panel-Cyber Security Working Group (SGIP-CSWG) – NIST
- Cyber Applied Research and Advanced Development – OSD
- Journal of Sensitive Cybersecurity Research and Engineering (JSCoRE) – ODNI

- **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 and long-lasting impact.
    - Testbeds and infrastructure for R&D – DARPA, DHS, DOE/OE, NSF, and OSD
    - Cyber Experimentation Environment, Cyber Measurement Campaign – OSD
    - Cyber Transition to Practice Program – DHS
    - Information Technology Security Entrepreneurs' Forum (ITSEF) – DHS
    - Secure and Trustworthy Cyberspace (SaTC) Program – NSF
    - Small Business Innovative Research (SBIR) Conferences – DHS and DoD
    - National Cybersecurity Center of Excellence (NCCoE) – NIST

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**: Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center – DHS and DOE/OE; Defense Technology Experimental Research (DETER) testbed – DHS and NSF; National Centers of Academic Excellence in Information Assurance Education and Research – DHS and NSA
- **Workshops**: Cybersecurity Applications and Technology Conference for Homeland Security – DHS; DoD Small Business Innovation Research (SBIR) Conference – DHS and DoD Service research organizations; 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; Workshops on Incorporating Security Concepts in Undergraduate Computer Science Curriculum – NSF; Workshop on Multi-spectrum Metrics for Cyber Defense – NSF; Human Dimension in Cyber Operations R&D Priorities Workshop – NSF and National Laboratories; Cybersecurity Insurance Workshop – DHS and NSF; IT Security Entrepreneur Forum, Innovation Summit, SINET Showcase, Transition To Practice Showcase – DHS; Science of Security Workshop – NSA and NSF; Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Industry Workshop – DHS and DOE/OE; Computational Cybersecurity in Compromised Environments (C3E) Workshops – ODNI
- **Collaborative deployment**: DNS security (DNSSEC) and routing security – AFRL, DHS, and NIST; NIST App Testing Portal (ATP) – DARPA and NIST; The National Vulnerability Database – DHS and NIST; U.S. Government Configuration Baseline (USGCB) – NIST and NSA
- **Interagency cooperation**: Ongoing information exchanges in support of developing a national cybersecurity R&D agenda – All
- **Technical standards**: Developing, maintaining, and coordinating validation programs for cryptographic standards – NIST and NSA; participation in Internet Engineering Task Force (IETF) security groups to develop standard representations and corresponding reference implementations of security-relevant data – NIST,

NSA, and OSD; Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) – NIST, DOE/OE

- **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 Science and Technology Priority Steering Council (Cyber PSC)**: 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 US-Israel Binational Science Foundation joint program; Network and Information Sciences International Technology Alliance (U.S. Army-United Kingdom collaborative program on secure data sharing and research collaboration among coalition partners); DHS International Engagements and co-funding with Australia, United Kingdom, Canada, Netherlands, Sweden, Germany, Israel, 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

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the CSIA PCA:

- **AFRL**: Secure systems foundations; foundations for trusted architectures; cyber agility (configuration-based moving target defense, polymorphic machines, polymorphic enclaves, IP hopping); cyber survivability and recovery (mission survival/recovery in the cloud, survive with mission assurance, recover with immunity), mission aware cyber C2 (engineering and requirements analysis, system M&S, integration and test environment, cyber defense components and applications projects); mission-centric cyber assurance (assure by design, mission assurance in the cloud)
- **ARL, ARO, and CERDEC**: Mobile security (tactical edge solutions for the dismounted warfighter); cyber maneuver (network and platform agility for mission assurance, cyber deception); cyber frameworks (capabilities built on open, sustainable and well-defined specifications and frameworks for defensive and offensive operations); trust research (trust management for optimal network performance, models and analytical tools for social-media-based data sensing and processing); intrusion detection (efficient and secure system for resilient defense, automatic signature generation); secure cross domain information sharing; software/hardware assurance (automated source code analysis, tamper and chip level protections); and cyber threat (novel methods and tools for prompt network protection); defensible cyber tactical cloud (cloud-based, virtual technologies for Army tactical environments that afford self-configuring, self-healing, and self-reporting properties); cyber maneuver (cognitive reasoning and feedback to maximize maneuver efficiency in tactical environments, predictive cyber threat modeling, dynamic OS maneuverability and application diversity)
- **DARPA**: Information Assurance and Survivability (core computing and networking technologies to protect DoD's information, information infrastructure, and mission-critical information systems; and cost-effective security and survivability solutions)

- **DHS**: Trustworthy cyberinfrastructure (internet measurement and attack modeling, process control system security, security for cloud-based systems, secure protocols – DNSSEC and RPKI/BGPSEC); cyber technology evaluation and transition (cybersecurity assessment and evaluation, cybersecurity experiments and pilots, transition to practice); foundational elements for cyber systems (software quality assurance, enterprise level security metrics and usability, Homeland Open Security Technology (HOST), cyber economic incentives, moving target defense, tailored trustworthy spaces); research infrastructure to support cybersecurity (experimental research testbed, research data repository, software assurance marketplace); 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. Collaborate with all energy sector stakeholders including national laboratories, academia, technology vendors, energy asset owners, and federal partners. Foster research in national labs and academia and engage in industry-led projects to transfer promising cybersecurity capabilities into the energy sector. Identify best practices and technologies for securing energy delivery systems by leveraging existing capabilities across the Federal Government and other Sector Specific Agencies. Continue to advance the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) that helps utilities to identify areas for cybersecurity investment, prioritize cybersecurity resources in a way that most effectively reduces risk, and compare their cybersecurity capabilities with other utilities
- **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; Tools for Recognizing Useful Signals of Trustworthiness (TRUST) Program
- **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; and supply chain risk management; participation in standards development organizations; National Cybersecurity Center of Excellence (NCCoE); National Strategy For Trusted Identities in Cyberspace (NSTIC); National Initiative for Cybersecurity Education (NICE); FISMA Phase II
- **NSA**: High assurance security architectures enabled by virtualization; improved enterprise protection through strong software measurement and reporting; secure enterprise infrastructure required for secure mobility; improved physical protection of mobile assets; location sensitive access control; cost-effective protection of air interface; integrating data from different sensors (host, LAN, gateway); non-signature based detection
- **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), Engineering (ENG), and the Office of Cyberinfrastructure (OCI)
- **ONR**: Software and cyber information assurance; trust management in service-oriented architecture; autonomic cyberinfrastructure (autonomic computing, and its components, automated discovery for cryptographic algorithms); controlling software complexity, predictability, security, and efficiency (automated complexity reduction, execution and latency predictability in multicore environments); proactive cyber network defense (ensuring continuity of cyber operations and availability of national assets during cyber conflict)

- **OSD**: 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; transition the leadership of the DoD Cyber Science and Technology Priority Steering Council (Cyber PSC) to AFRL; cyber security metrics; and SBIR workshop to facilitate networking with small businesses

High Confidence Software and Systems (HCSS)

NITRD Agencies: DARPA, DHS, DoD Service Research Organizations, DOE/OE, NASA, NIH, NIST, NSA, NSF, and OSD
Other Participants: ARPA-E, DOT, FAA, FDA, FHWA, JPDO, NRC, NTSB, USDA, and VA

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 2014 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 health care, 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 a public domain, cyber-physical testbed
- **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 new integrated analytical and decision-support tools; develop Engineered Resilient Systems (ERS); 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" 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 engages both the physical and cyber disciplines and fosters 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 2014. 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 – DoD Service research organizations, DOE/OE, 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, DOE/OE, FDA, NASA, NIH, NIST, NSA, NSF, ONR, and OSD

- **High-confidence systems in the energy sector**: Continue the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) to help utilities identify and prioritize areas for cybersecurity investment and compare cybersecurity capabilities across utilities; continue work with the national laboratories on high-risk/high-payoff research that aligns with energy sector needs; continue support for the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) academic collaboration that brings expertise in power system engineering and the computer science of cybersecurity to the research and development of energy delivery systems that sustain critical functions during a cyber-event – DHS, DoD, DOE/OE, and NIST
- **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 – DOE/OE, 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, JPDO, and NASA
- **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; 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, JPDO, 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 of workshops and other research meetings that bring a broad mix of stakeholders together who might not otherwise cross paths. 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 first-of-their-kind 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** – Spring 2013 Workshop on "Medical Device Innovation Using Cyber Physical Systems" – FDA, NIST, NSA, and NSF
    - **Future Energy CPS** – DOE/OE, NIST, NSA, and NSF

  - **High Confidence Transportation CPS**: Automotive, Aviation, and Rail – AFRL with DOT, FAA, FDA, NASA, NIST, NSA, NSF, and NTSB
  - **CPS Week** – High Confidence Networked Systems (HiCoNS) – AFRL, NASA, NIST, NSA, and NSF
  - **Verified Software, Theories, Tools, and Experiments (VSTTE) Workshop** – 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
  - **CPS Extreme Manufacturing**: FDA, NIST, 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)**: AFRL, NASA, NSA, and NSF
- **13th Annual HCSS Conference**: Showcasing of promising research to improve system confidence – FAA, NASA, NSA with NSF, ONR, and OSD
- **Software Assurance Forum** – DHS, DoD Service research organizations, NIST, NSA, and OSD
- **Safety of flight-critical systems**: Workshops and technical discussion – AFRL, NASA, NSA, and NSF
- **Future Directions in Cyber-Physical Systems Security**: Joint workshop – DHS, DOE/OE, NIST, NSA, NSF, OSD, and USAF
- **Standards, software assurance metrics for Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS)**: Collaborative development – DOE/OE, NIST, and others
- **Biomedical imagery**: Technical standards for change measurements in patient applications – CMS, FDA, NIH, and NIST
- **Cooperative proposal evaluation** – AFRL, FAA, FDA, NASA, NIST, NRC, NSA, NSF, and OSD
- **FAA National Software and Airborne Electronic Hardware Standardization Conference** – FAA and NASA
- **"The New Clockwork for Time-Critical Systems" workshop report**: HCSS agencies
- **Foundations of CPS conferences** – NIST and NSF
- **Interagency collaboration on cybersecurity and power grid**: Collaboration among Trustworthy Cyber Infrastructure for the Power Grid, Electricity Subsector Cybersecurity Risk Management, and Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) – DHS, DOE/OE, and NIST
- **5th NASA Formal Methods Symposium (NFM 2013)** – AFRL, DARPA, FAA, FDA, NASA, NIST, NSF, and NSA
- **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 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the HCSS PCA:

- **AFRL**: R&D in improved system design methodologies and enhanced V&V techniques supporting safety and security airworthiness certification of onboard embedded, flight-critical aircraft systems operating in a system-of-systems environment, e.g., UAVs; and emphasis on mixed-criticality (i.e., air safety combined with security) interdependencies requiring deep interaction and integration of hardware and software components
- **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. Collaborate with all energy sector stakeholders including national laboratories, academia, technology vendors, energy asset owners, and federal partners. Foster research in national labs and academia and engage in industry-led projects to transfer promising cybersecurity capabilities into the energy sector. Identify best practices and technologies for securing energy delivery systems by leveraging existing capabilities across the Federal Government and other Sector Specific Agencies. Continue to advance the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) that helps utilities to identify areas for cybersecurity investment, prioritize cybersecurity resources in a way that most effectively reduces risk, and compare their cybersecurity capabilities with other utilities
- **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/flight-data recording and analysis
- **FHWA**: Apply concept of cyber-enabled discovery and innovation to develop new transportation paradigm for an Integrated Active Transportation System (IATS) focused on three major technical areas: autonomous transportation system beyond-autonomous vehicle system, real-time response (prediction, prevention, control), and advanced emergency response; the goals are to develop new energy sources and reduce emissions, reduce accident frequency and achieve zero fatality, increase mobility and reduce congestion, improve national productivity and economy, and drive national competitiveness in science and technology
- **NASA**: Aviation safety R&D with emphasis on enabling technologies for design, V&V of flight-critical systems (argument-based safety assurance, autonomy and authority, integrated distributed systems, software-intensive systems); enabling assurance technologies for NextGen self-separation concepts; and determining appropriate airworthiness requirements for UAS to help enable routine access to the national airspace
- **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**: Computer forensics tool testing; National Software Reference Library (funded by DOJ/National Institute for Justice [NIJ]); 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; and automotive CPS
- **NRC**: Regulatory research to assure safety and security in cyber-physical systems (digital instrumentation and control systems) used in the nuclear energy sector
- **NSA**: High-assurance system construction (correct-by-construction methods, model-driven development, programming languages) and analysis (concolic execution, multi-tool analysis, separation/matching logic, static/dynamic analysis); 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; Trustworthy Computing (TwC) to ensure security, reliability, privacy, and usability; create core disciplinary, exploratory, and educational programs; and the 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 agency mission needs and support national competitiveness. The HEC infrastructure enables researchers in academia, industry, and federal laboratories to model and simulate complex processes in aerospace, astronomy, biology, biomedical science, chemistry, climate and weather, energy and environmental sciences, high energy physics, materials science, nanoscale science and technology, national security, and other areas to address national priorities and federal agency mission needs. HEC technologies impact the entire spectrum of computing devices, from the largest systems to hand-held devices, allowing larger computing platforms to become more affordable and smaller devices more powerful over time. The federal HEC infrastructure also serves as a critical enabler of initiatives associated with emerging national priorities such as big data, nanotechnology, the Materials Genome Initiative, and advanced manufacturing.

President's FY 2014 Request

Strategic Priorities Underlying this Request

Investments in federal HEC facilities, advanced applications, and next-generation systems support national competitiveness in advanced technologies and provide the means for industry, academia and federal laboratories to apply advanced computational capabilities in support of federal agencies' existing 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-quality HEC systems**: Provide HEC systems with capabilities needed to meet critical agency mission needs and support the national science and engineering communities, US industry, and academic research; ensure that emerging computer technologies support industrial, national security, and scientific applications and reduce energy requirements for computing technology at all scales. US leadership in HEC systems enables US competitiveness
- **Advancement of HEC applications**: Support the development of 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 for emerging architectures
- **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 laboratories; 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 cross-cutting 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 2014 under each of the main HEC I&A priorities. Agencies are listed in alphabetical order:

- **Leadership-class and production-quality HEC systems**
  - **DoD (HPCMP)**: Deployment of new HEC systems (petascale) in response to evolving computational requirements from the DoD S&T and T&E communities; mature and demonstrate state of the practice compute environments in support of DoD RDT&E and acquisition engineering communities with a focus on productivity for non-traditional users
  - **DOE/NNSA**: Common capacity hardware and software environment across LANL, LLNL, and SNL
  - **DOE/SC**: National Energy Research Scientific Computing Center (NERSC)-7 delivery; operate 27 PF system at the Oak Ridge Leadership Computing Facility and a 10 PF system at the Argonne Leadership Computing Facility
  - **NASA**: At NASA Advanced Supercomputing facility (NAS), conduct NAS Technology Refresh (NTR) to select and install next-generation, multi-PF HEC technology to meet growing computational demand for aerospace, earth science, and astrophysics; and augment NASA Center for Climate Simulation (NCCS) resources for increased model resolution and complexity, large-scale observational data analysis, and satellite observations for climate model comparisons
  - **NIH**: Continued support for broad-based HEC I&A for biomedical computing applications. Selected acquisition of cluster and mid-scale compute-intensive HEC systems
  - **NOAA**: Continue to operate SGI ICE (383 TF) for weather and climate research; and operate 1,100 TF GAEA climate research system at ORNL
  - **NSF**: Capacity Systems: Track 2 resources - Kraken extended to May 2014, Lonestar and Blacklight extended one year, Ranger discontinued; Gordon and Keeneland are allocatable resources under XSEDE; Stampede operations (2 PF of Sandy Bridge CPU, 8 PF of Intel Many Integrated Cores (MIC) accelerators provide shared services via XSEDE and TIS projects, with 1K+/year research projects planned; Capability System: Blue Waters system operational, providing sustained petascale computational performance to 30+ science and engineering teams (Cray XE/XK 6, >1 PF sustained, 11.5 PF peak performance, 1.5 PB aggregate system memory, 25 PB user accessible file storage)
- **Advancement of HEC applications**
  - **DoD (HPCMP)**: Multi-physics applications development, verification and validation for acquisition engineering community; training and university technology transfer; computational tools development; S&T application modernization
  - **DOE/NNSA**: Explore code transition/re-write options for exascale readiness via co-design; investigate embedded UQ methodologies for multicore architectures
  - **DOE/SC**: SciDAC institutes for frameworks, algorithms, and scalable technologies, including data management, analysis, and visualization; applied mathematics research (new math centers, UQ at extreme scale computations, resilient solvers); exascale co-design centers for next generation applications (LANL, ANL, SNL); FastForward research and R&E prototypes expanded to fill gaps and address challenges and opportunities presented by emerging new computer architectures
  - **EPA**: Advanced distributed data and modeling capabilities to support Air Program goals; applications, analytics, and infrastructure for robust mission-related modeling and research in air quality, climate, and interactions with human health
  - **NASA**: Application enhancement, data analysis, data management and visualization support for advanced modeling in aerospace, earth science, and astrophysics; summer institute to train discipline experts in efficient, scalable parallel programming

- **NIH**: Scientific computing efforts such as biomolecular modeling, physiological modeling, and multiscale modeling that use HEC resources or are in pre-HEC state; biodata management and analysis
- **NIST**: Measurement science for HEC applications (properties of materials from first principles, design of experiments); visualization (uncertainty quantification, calibration and correction, quantitative methods in visualization); accelerate development and industrial applications of advanced materials (Materials Genome Initiative)
- **NOAA**: Improve model-based computing of weather forecasting, hurricane forecasting, and climate prediction; ensemble forecasts, ecosystem forecasting, and integration with physics-based modules, hybrid architectures
- **NSF**: Continue XD program for four more years; software strategies for S&E and education, advance and sustain software infrastructure, and address software lifecycle

- **Leading-edge cyberinfrastructure**
  - **DoD (HPCMP)**: Continue development of nationwide high bandwidth, low-latency R&D network; collaborative development of cybersecurity tools; frameworks for productivity of non-expert users to enable broader application of HEC-enabled solutions
  - **DOE/NNSA**: Develop common computing environment across NNSA labs
  - **DOE/SC**: Continue emphasis on unified approaches to software, languages, and tools support to reduce barriers to effective use of complex HEC resources by application developers and users
  - **NASA**: Collaborate with industry to evaluate future advanced HEC system architectures for NAS; collaborate with DOE to develop NCCS Data Management System to support data analysis; and demonstrate new approaches for distributed, data-intensive computational science and engineering, including cloud-like HEC services
  - **NIH**: Continue investment in scientific computing, e.g., software development; neuroscience/BISTI solicitations, grid computing
  - **NOAA**: Leverage existing nationwide high-bandwidth, low-latency network to promote shared use of high performance computing across agencies
  - **NSF**: CIF21 – Meta-program to coordinate the full cyber-ecosystem across NSF, advancing science and engineering through foundational research for managing, analyzing, visualizing, and extracting knowledge from massive datasets; SI^2 – long-term investment focused on catalyzing new thinking, paradigms, and practices in developing and using software, creating a software ecosystem that encompasses all levels of software and spans from embedded sensors to HEC to major instruments and facilities

Planning and Coordination Supporting Request

Since 2005, the HEC agencies have provided tens of billions of compute 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. Another key focus is selecting, evaluating, procuring and operating federal high-end platforms – a complicated, labor-intensive process in which 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 HEC systems**
  - **Access to leadership-class 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, DOE/NNSA, DOE/SC, NASA, NOAA, NSA, and NSF
  - **NSF review of supercomputing facilities**: DOE/SC and NSF
- **Advancement of HEC applications**
  - **DOE intra-agency collaborations**: SciDAC 3 institutes and partnerships – DOE/SC
  - **Multiscale modeling in biomedical, biological, and behavioral systems**: Interagency collaboration to advance modeling of complex living systems – DoD, NIH, and NSF
  - **INCITE**: Award of five billion core hours, from requests for > 14 billion hours; study of flow of suspensions and distribution of grid partitioning code – DOE/SC and NIST
  - **Computational toxicology**: Integration of HEC technologies with molecular biology to improve methods for risk assessment of chemicals – DoD, DOE/SC, EPA, FDA, and NIH
- **Leading-edge cyberinfrastructure**
  - **Automated combinatorial testing of software systems**: Methodology and infrastructure for automated testing that reduces the number of tests – NASA and NIST
  - **Remote sensing information gateway**: Allows users to integrate selected datasets into unified visualization, accessing key environmental models and data – DOE/SC, EPA, NASA, and NOAA
- **Broadening impact**
  - **Interagency participation in proposal review panels, principal investigator meetings** – HEC agencies
  - **DOE best practices workshop series:** Develop and share best practices for HEC operations – DOE/NNSA, DOE/SC, and HEC agencies
  - **Competitiveness**: Broaden use of HEC and advanced modeling and simulation by U.S. engineering and manufacturing industries to expand advanced manufacturing capabilities across small, medium, and large business sectors – HEC IWG
  - **Education/workforce development**: Infuse 21st century curriculum in HEC and computational science into academia and define a framework for development of the existing workforce, that addresses HEC skills for both next-generation providers and users of HEC, based on federal HEC agency requirements – 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

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the HEC I&A PCA:

- **DoD (HPCMP)**: HEC services for R&D and test communities (e.g., platforms, computational science software support); computational science institutes for DoD priorities (air armament, health force protection,

weather prediction, ground sensors, space situational awareness, rotorcraft, networks, microwaves, and munitions)

- **DOE/NNSA**: Operate ASC Cielo system (1.3 PF) at LANL and Sequoia system (20 PF) at LLNL; prepare and execute next round of commodity technology systems procurement
- **DOE/SC**: Manage LCF facilities at ORNL (27 PF) and ANL (10 PF); initiate the >10 PF (peak) NERSC-8 upgrade advanced conceptual design; support computation-intensive and data-intensive applications; programming environment challenges; mathematics for complex systems
- **NASA**: Explore distributed, data-intensive, and energy-efficient technologies for enhanced user productivity; complete current cycle of NAS and NCCS technology refresh and system upgrades
- **NIH**: Fund predominantly broad-based biocomputing awards; implement recommendations, as directed, based on the Final report to The Advisory Committee to the Director, NIH, by the Data and Informatics Working Group
- **NIST**: Parallel and distributed algorithms (computational modeling of suspension; nanostructures; computation of properties of atoms and molecules; Object-Oriented Micromagnetics Modeling Framework [OOMMF]; quantum key error correcting codes; human language technology; pattern recognition); fundamental mathematical tools (Parallel Hierarchical Adaptive Multi-Level solver [PHAML]; rapid evaluation of integrals in high precision calculations); Virtual Measurement Laboratory (immersive and desktop visualization – systems, applications, interfaces and visualization)
- **NOAA**: Detailed design and planning for next-generation NOAA research HPC architecture
- **NSF**: CIF21, software- and data-enabled science; CPS; advanced manufacturing; cybersecurity; computing workforce; high performance computing and storage services; XD remote visualization and data analysis services; technical audit service; technical insertion service; XSEDE integrating services (coordination and management service, extended collaborative support service, training, education, and outreach service); migrate Track 2D (FutureGrid, Keeneland, Gordon) to XSEDE allocatable resources

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

NITRD Agencies: DARPA, DoD Service Research Organizations, DOE/NNSA, DOE/SC, NASA, NIH, NIST, NOAA, NSA, NSF, and OSD

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 to support national competitiveness and to meet 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 across computational platforms at all scales. Research areas of interest include quantum information science; system software and system architectures that effectively utilize billion-fold concurrency; reducing the energy per computation by orders of magnitude; achieving system resilience at extreme scales; and enabling future revolutions in simulation and big-data-enabled science and technology.

President's FY 2014 Request

Strategic Priorities Underlying This Request

For decades, HEC R&D agencies have led development of increasingly capable computing technologies and environments 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 and scientific leadership. Now, the HEC community faces great challenges in creating effective high-end systems using technology that is driven by the consumer marketplace, requiring advances in energy utilization, data movement, concurrency, resilience, and programmability. These challenges must be met to achieve and exploit the orders of magnitude increase in HEC capability that are needed by 2020 to solve increasingly complex and data-intensive problems for science, engineering, and national security. To address the growing complexity and long-term costs of emerging platforms, HEC researchers seek to exploit multicore-processor technologies, novel memory and storage technologies, and innovative approaches to software creation, and to innovate despite the challenges of energy consumption, reliability, and scalability. Given these challenges and a closing window for influencing chip designs, the HEC R&D agencies see the following as key research priorities for FY 2014:

- **Extreme-scale computation**: Integrate computer science and applied mathematical foundations to address the challenges of productive and efficient computation at the exascale level and beyond. Develop innovative systems that combine increased speed, efficient use of increasingly scarce sources of energy, 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. Explore new concepts and approaches for solving technical challenges such as power use, thermal management, file system I/O latency, resiliency, highly parallel system architectures with support for billion-way concurrency, and programming language and development environments that can increase the usability and utility of large-scale multiprocessor (including hybrid) systems. Develop, test, and evaluate prototype HEC systems and software to reduce industry and end-user risk and to increase technological competitiveness
- **New directions in HEC hardware, software, computer science and system architectures**: Develop novel scientific frameworks, power-efficient system architectures, programming environments, and prototypes to take computing power and communications "beyond Moore's Law" and to advance quantum 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 software to

enable, support, and increase the productivity of geographically dispersed collaborative teams that develop future HEC applications

- **Broadening impact**: Conduct cross-cutting 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

Highlights of the Request

The HEC R&D agencies report the following areas as highlights of their planned research investments for FY 2014 under each of the main HEC R&D priorities. Agencies are listed in alphabetical order:

- **Extreme-scale computation**
  - **DOE/NNSA:** Investments in identified R&D critical technologies to address exascale barriers via FastForward collaboration with DOE/SC
  - **DOE/SC**: Computer science research, including abstract machine models and performance models to guide design and development of future exascale machines that generate and exploit massive data
- **New directions in HEC hardware, software, computer science, and system architectures**
  - **DARPA**: Power efficient processing for embedded computing
  - **DOE/SC**: Computer science and applied mathematics research, including programming environments; self-aware runtime systems to exploit resources through dynamic adaptive resource management and task scheduling; innovative operating systems for scalability, energy and reliability management, resource allocation and recovery, efficiency and protection; architectures for cores and systems to minimize latencies, preclude bottlenecks, reduce energy of data movement and control; address interrelated challenges of energy utilization, data movement, resiliency, concurrency, and programmability; invent scalable methods to manage, analyze, and visualize data at extreme scales
  - **NIST**: Quantum computing, including quantum information theory and science; architectures and algorithms; modeling of quantum memory, components, and systems; techniques and tools to assess the capabilities of candidate technologies; technology demonstrations
  - **NSA**: ACS research program; superconducting; quantum computing
  - **NSF**: GENI – a prototype virtual laboratory for exploring next-generation internets and distributed computation, storage, and networking
- **Productivity**
  - **DoD, DOE, and NSF**: Capabilities for scientific research - computational concepts, methods, and tools for discovery. Centers, institutes, and partnerships for predictive and data-intensive science, applied math and computer science challenges of scientific computing at extreme scale, joint mathematics and computer science institutes

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 exascale resilience**: DoD, DOE/NNSA, and DOE/SC
  - **DOE intra-agency collaborations**: Computing MOU; FastForward investments in memory, processors, storage; joint system procurements for next advanced technology systems delivered in 2015 and 2017 – DOE/NNSA and DOE/SC
- **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, NIST, NSA, and NSF
  - **DOE intra-agency collaborations**: Joint development of DOE Exascale Strategy to address fully the parallelism, power, memory, and data movement issues associated with multicore computing at the exascale level – DOE/NNSA and DOE/SC
  - **Exascale system software R&D co-funding**: DoD (HPCMP), DOE/NNSA, and DOE/SC
  - **3D stacked memory project**: DOE/NNSA and DOE/SC
- **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 – DoD, 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
- **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, DOE/NNSA, DOE/SC, NASA, NSA, and NSF
  - **HEC data challenges**: Coordinate with HCI&IM CG, LSN CG, Big Data SSG, and IWG on Digital Data – Multiple HEC agencies
  - **Workforce development planning**: HEC IWG and NITRD SEW-Ed agencies
  - **ASCR Committee of Visitors Review of Computer Science program**: DOE/SC and NSF

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the HEC R&D PCA:

- **DARPA**: Develop the technologies and techniques to overcome the power efficiency barriers that currently constrain embedded computing system capabilities
- **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**: Exascale Research Conference, promoting interagency U.S. Government/industry collaboration and integration of multiple lines of exascale research; International Exascale Research Conference, promoting global collaboration among exascale researchers; SciDAC 3 Principal Investigator meeting; Data Intensive Science Workshop; Exascale Operating and Runtime Systems workshop and FOA; Storage Systems and I/O Workshop and FOA
- **NASA**: Advanced HEC technologies for enhanced productivity, emphasizing efficient computing, integrated environments, and ultrascale computing
- **NIST**: Quantum information theory (algorithms for simulation of quantum field theories; analysis of quantum complexity classes); quantum computing assessment (benchmarks for testing fidelity of multi-qubit gates; procedures to assess the fidelity of generated quantum states); quantum technology demonstrations (memory technologies and specialized quantum devices)
- **NOAA**: Modeling of the earth system (e.g., ESMF), large-scale data transfer, optimizing configuration for grid computing and meta scheduling, and transitioning code from research to operations
- **NSA**: ACS research program changed from thrust-centric to end-end centric for modeling, simulation, emulation; computer architecture and engineering; mission proxies; system level metrics (energy, productivity, resilience); SME collaborations (machine learning, file I/O, runtime systems, memory and storage, etc.)
- **NSF**: CIF21; software- and data-enabled science; CPS; advanced manufacturing; VOSS activities; robotics; energy independence; computing workforce; smart health and wellbeing

Human Computer Interaction and Information Management (HCI&IM)

NITRD Agencies: AHRQ, DARPA, DHS, DoD Service Research Organizations, DOE/SC, EPA, NARA, NASA, NIH, NIST, NOAA, NSF, ONC, and OSD
Other Participants: IARPA, USDA, USGS, and VA

HCI&IM focuses on R&D to expand human capabilities to use and manage data and information through the use of computer hardware, software, and systems technologies. These technologies include robotics, visualization agents, cognitive systems, collaborative systems, and others that support the organization and the journey from data to knowledge to action. Scientific research, energy and the environment, climate change and prediction, healthcare, education and training, protecting our information infrastructure, emergency planning and response, national defense, homeland security, weather forecasting, and space exploration are just some of the national priorities that HCI&IM research helps facilitate and improve.

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). As exemplified in the National Big Data R&D Initiative launched in March 2012, transformative approaches for accessing and extracting meaning from data has become 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 2014 Request

Strategic Priorities Underlying This Request

Strategic priorities in HCI&IM include:

- **Human 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 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
- **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 for data to be brought together with shared meaning, providing the basis for interoperability and relationship building which is a basic step of 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 2014. 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, DOE/SC, EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and OSD
- **Human engagement and decision**: 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, NSF, and OSD
- **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 – DOE/SC, EPA, NARA, NASA, NIH, NIST, NOAA, and NSF
- **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 SSG 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, CMS, 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 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; affective computing – DARPA, DoD Service research organizations, NASA, NIST, NSF, and OSD
- **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, NSF, and OSD

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:

- **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* – 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, OSD, 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 participate in the IWG on Digital Data and the IWG on Public Access to Scientific Publications. Topics of consideration include new policy development and identification of existing standards for interoperability, such as the Digital Preservation Interoperability Framework International Standard (DPIF) – EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies
- **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 – AHRQ, DHS, EPA, NARA, NASA, NIH, NIST, NOAA, NSF, and other agencies
- **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, NSF, and ONC

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the HCI&IM PCA:

- **AHRQ**: Quality measurement and improvement; healthcare decision making; patient and clinician information needs; and U.S. Health Information Knowledgebase
- **DARPA**: Automatically translate large volumes of foreign-language speech and text, including informal genres; enable automated extraction, processing, and inference of information from text in any application domain
- **EPA**: Databases for computational toxicology; scientific information management (tools, best practices for management, accessibility of complex EPA data sets); and distributed environmental applications
- **NARA**: Global-scale capable, open source, "next generation" cloud 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**: Human-centered automation concepts for aviation safety; basic and applied research in human performance; decision-support technologies for NextGen; multimodal interface research; applied information systems research to help increase productivity of scientific research; research on advanced tools for discovering tools and services, and developing as well as preserving provenance of data products and associated information
- **NIH**: Basic research relating to biomedical informatics, computational modeling simulation, and human-computer interaction and information use funded under the Biomedical Information Science and Technology Initiative (BISTI); Basic Behavioral and Social Science Opportunity Network (OppNet), NLM Express Research Grants in Biomedical Informatics, and other individual or collective initiatives; 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 metrology, standards; usability of voting and security systems; 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; Hurricane Research Division (HRD) Forge centralized database for hurricane data, models; disaster planning, mitigation, response, and recovery
- **NSF**: Through academic R&D, NSF supports CIF21 as well as programs in support of information privacy, ubiquitous networked data environments, human-computer partnerships, socially intelligent computing, universal access, cognition mechanisms in human learning, and remote access to experimental facilities

Large Scale Networking (LSN)

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

LSN members coordinate federal agency networking R&D in leading-edge networking technologies, services, and enhanced performance, including programs in fundamental networking research, future Internet architectures, heterogeneous multimedia testbeds; middleware; end-to-end performance and performance measurement; network security; software defined networks, wireless networks, and networks for disaster response; the science and engineering of complex networks; networking tools and services for cloud, grid, and collaboration; advanced networking components; networking education, training, and outreach; and the engineering and management of large-scale networks for scientific and applications R&D, including capabilities for large-scale data transfer and virtual organization functionality. The results of this coordinated R&D, once deployed, assure that the next-generation Internet will be scalable, reliable, and flexible.

President's FY 2014 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 collaboration capabilities with demanding constraints of end-to-end performance, security, reliability, and availability. The advanced federal research networks support national security needs as well as transport data among the world's leading science discipline 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 performance measurement activity, for example, is enabling federal researchers to monitor and improve end-to-end performance across multiple network domains, and facilitating adoption of innovative capabilities in the marketplace. LSN collaborative activities for 2014 will focus on:

- **Enabling end-to-end big data applications:** Identify architectures, technologies, campus interfaces, and best practices for implementing and integrating end-to-end networking and storage for big data applications
- **Operational capabilities:** Identify approaches, best practices, and testbed implementations for Software Defined Networking (SDN)/OpenFlow, tactical communications and network technologies (e.g., dynamic ad-hoc, multi-hop wireless networks and data-centric environments), identity management, cloud computing, collaboration capabilities, spectrum management, IPv6, DNSSEC, science DMZ, and Trusted Internet Connections (TICs). Promote cooperation among network R&D testbeds and applications development including GENI, ANI, US Ignite, and others
- **Optical networking**: Coordinate the development and deployment of dynamic optical networking to support leading-edge science applications (e.g., technology, architecture, and infrastructure), 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 2014. Agencies are listed in alphabetical order:

- **Network architectures and protocols for future networks**: Develop and test network architecture concepts to enable reliable, secure, flexible, dynamic, heterogeneous networking and hybrid networking capabilities, and support sustainable environments, energy-efficient networking, and virtualization at scale – AFRL, CERDEC, DARPA, DoD (HPCMP), DOE/SC, NASA, NIST, NSF, and ONR

- **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, Coronet, Online Representations and Certifications Application (ORCA), SATCOM-CX, InfiniBand single-stream flows over wide area networks (WANs) – DOE/SC, NASA, NOAA, NSF, and OSD
- **Experimental network facilities**: Provide testbeds at differing scales, promote cooperation, and test advanced applications on DOE/SC's 100 Gigabit (Gb) ANI, NSF's GENI and other R&D testbeds, to demonstrate performance at scale of new architectures (e.g., SDN and OpenFlow), end-to-end applications (e.g., US Ignite) and protocols – DOE/SC, NASA, NIST, NOAA, and NSF
- **Strategic technologies for networking**: Provide basic research, development, and demonstration of new technologies for robust, secure, reliable, evolvable, wired and wireless networking for autonomous dynamic ad hoc routing infrastructure, tactical networking, autonomous cars, intelligent (efficient) buildings, medical devices, and assistive technologies – CERDEC, DARPA, DOE/SC, NIST, and NSF
- **Scientific collaboration capabilities:** Develop, provide, and manage software, tools, and infrastructure to support advanced science collaboration spaces and infrastructures – AFRL, CERDEC, DOE/SC, NASA, NIST, NSF, and ONR
- **Cloud and grid computing**: Secure federated software tools and cloud services for cyber-physical systems, data distribution and management, visualization, software stack for large-scale scientific collaborations, high-bandwidth implementation, interoperable smart grid standards and testbeds, Open Science Grid, Worldwide Large Hadron Collider Computational Grid, Earth System Grid – 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, and modeling for economic sustainability – AFRL, CERDEC, DOE/SC, NSF, and ONR
- **Networking for health science research, clinical needs**: AHRQ, NIH, NIST, and NSF
- **End-to-end network management, performance measurement**: Enable cross-domain end-to-end performance measurement for advanced networking; autonomous secure management; provide tools for and implement Performance Services-Oriented Network Architecture (perfSONAR, fault tolerance – CERDEC, DOE/SC, NASA, NIST, and NSF
- **Computational research infrastructure**: Provide networking to support U.S. and international research communities for networking research, large-scale data flows, and applications across all science disciplines – DoD, DOE/SC, NASA, NIH, NIST, NOAA, and NSF
- **Security implementation and research (IPv6, DNSSEC, and Trusted Internet Connections [TICs]):** Develop and implement near-term mandated capabilities – DHS, DOE/SC, NASA, NIH, NIST, NSF, and OSD
- **Network security research**: Develop technologies for detection of anomalous behavior; standards, modeling, and measurement to achieve end-to-end security over wireless networks, heterogeneous, multidomain networks and infrastructure; critical-infrastructure protection; trustworthy networking; privacy, confidentiality, authentication, policy; delay tolerant networking; and cryptography – AFRL, CERDEC, DARPA, DOE/SC, NASA, NIH, NIST, NSF, ONR, and OSD
- **Complexity in networking:** Develop concepts, methods, architectures, protocols, and measurement for modeling networks as complex, autonomous, and dynamic systems – DARPA, DOE/SC, NIST, and NSF
- **Wireless networking**: Develop standards, tools enabling better interconnectivity; seamless domain, heterogeneous, and layer interoperability; and management (e.g., power, data fusion, heterogeneous interfaces, spectrum sensing and sharing, mobile hotspots, constraints and efficiency, under harsh

conditions) for robust, secure, dynamic, mobile and sensor networks – CERDEC, DARPA, NASA, NIST, NSF, ONR, and OSD

- **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 to resolve technical networking issues at the global level and to develop collaborative testbeds for exploring advanced technologies at scale. In summary, the following are ongoing LSN coordination activities:

- **Interagency research agenda**: Workshops on networking for extreme-scale science and data flows; experimentation, network management, smart grid, DETER, perfSONAR deployment; experimental design for complex systems; and network performance measurement – LSN agencies
- **Infrastructure cooperation**: National and international connectivity – DoD, DOE/SC, NASA, NOAA, and NSF
- **Multiagency workshops**: Leveraging perfSONAR and implications for Internet instrumentation research; semantically rich descriptions of networked systems – Multiple agencies
- **Transoceanic networking for science** – DOE/SC and NSF
- **Inter-service collaboration**: Services for federation, management, information, discovery, and delivery – AFRL, CERDEC, and ONR
- **Software defined networking:** Testing of SDN and OpenFlow applications in at-scale testbeds – DoD, DOE/SC, NIST, NSF, and NSA
- **Coordination by LSN Teams**
    - **Joint Engineering Team (JET)**: Advanced testbeds, coordination of end-user requirements, science user interfaces, engineering of research networks and testbeds (JETnets); big data and storage networks; security best practices, applications testbeds (DNSSEC, IPv6, performance measurement), TICs coordination; interdomain and end-to-end metrics, monitoring; tool sharing and exchange; international coordination; and transit and services cooperation – DoD (HPCMP), DOE/SC, FAA, NASA, NIH, NIST, NOAA, NSA, NSF, ONR (NRL), and USGS
    - **Middleware And Grid Interagency Coordination (MAGIC) team**: Cloud computing services, grid computing services, middleware; cloud and grid standards and implementation status (TeraGrid, Open Science Grid [OSG], Earth Systems Grid [ESG]); security and privacy, e.g., identity management; and international coordination – AFOSR, DOE/SC, NASA, NIH, NIST, NOAA, and NSF
- **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 – AFRL, DARPA, DHS, DOE/SC, NASA, NIST, NSA, and NSF
- **Partnerships for research connectivity** – DOE/SC, DoD (HPCMP), NASA, NOAA, and NSF

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 under the LSN PCA:

- **AFRL**: Tactical airborne links and networks, global, interference tolerant, spectrum efficient agile networks, wideband hybrid optical/RF communications, cross-domain information sharing, tactical wireless, secure multidomain collaboration, mission responsive information services
- **AHRQ**: With CMS - Children's Health Model EHR Format; with CMS, ONC, NIH (NLM) - United States Health Information Knowledgebase (USHIK)
- **CERDEC**: Multilayer network analysis/network optimization, end-to-end flow management, spectrum management, operations in contested spectrum environments, network resilience, policy-based network and spectrum management, Joint Cognitive Network Radio Testbed, Virtual Ad hoc Network testbed (VAN)
- **DARPA**: Mobile wireless communication systems and networks; increased network capacity and scaling; spectrum efficiency in congested spectrum; network degradation tolerance; electromagnetic interference mitigation; counter network reconnaissance and surveillance; and counter denial of service
- **DoD (HPCMP)**: Multidomain performance measurement; SDN/OpenFlow development/demonstration; DREN; IPv6, DNSSEC, TICs; cybersecurity defenses; and network high-speed access to Alaska and Hawaii
- **DOE/SC**: SDN/OpenFlow, energy-aware networking for big data infrastructures, complex network end-to-end models and simulations, advanced collaboration spaces for exascale science, extreme-scale scientific collaboration spaces and infrastructure, end-to-end testing of advanced applications on 100 Gbps networks, multiple 100 Gbps lambdas for big data transfers, big data flows across domains (science DMZ - network architecture to bypass campus firewalls, enabling large-scale data transfers while minimizing impacts on local network applications), open exchange points (layers 1, 2, and 3), trans-Atlantic 100 Gbps lambdas
- **NASA**: Network access control, end-to-end QOS, TIC security monitoring, IT security, emerging technology, enterprise architecture, management governance, IPv6 transition, web proxies, and intrusion protection
- **NIH**: Healthcare IT, infrastructure creation and applications: BIRN, DIMRC, NCBC, CBIIT; with NSF - TeraGrid, CIF21; collaborative research in computational neuroscience, core technology for big data science and engineering
- **NIST**: Measurement science for complex systems; Internet infrastructure protection, public safety communications; personal and medical devices models and standards, smart grid, and seamless cloud computing
- **NOAA**: N-Wave integration of and access to HPC and data centers, TICs, measurement and performance tools, preparation for 100 Gbps networking, next generation of Next Generation Internet Exchange (NGIX), shared network infrastructure including access to Alaska and Hawaii
- **NSA**: Delay-tolerant networking, enhanced security, secure architectures for cloud computing, IPv6 enhanced security
- **NSF**: Core and strategic networking research (NeTS); economic sustainability of networks, spectral efficiency, spectrum sensing, reconfigurable wireless platforms; applications over reconfigurable network architectures at scale (GENI); Enhancing Access to Radio Spectrum (EARS); US Ignite (public sector Gbps applications for national priorities); education and outreach; Cyberinfrastructure for 21st Century Science and Engineering (CIF21), cloud enablement of cyber-physical systems; social-computational systems; middleware; performance-monitoring capabilities; international infrastructure (International Research Network Connections [IRNC]); Cyber-Enabled Sustainability Science and Engineering (CyberSEES); Campus

Cyberinfrastructure-Network Infrastructure and Engineering (CC-NIE); Secure and Trustworthy Cyberspace (SaTC)

- **ONR**: Robust interference alignment, optimal distribution with access, security, robustness to failures, distributed synchronization, control of heterogeneous wireless networks, dynamic, robust routing under harsh conditions, autonomous network management

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

NITRD Agencies: DHS, DOE/NNSA, DOE/SC, NASA, NIH, NIST, NSF, ONR, and OSD
Other Participants: ED

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 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 2014 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 are taking place in 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:

- **Promote understanding and support for collaboration**
  - **IT-enabled innovation ecology**: Shape the creation of IT and research on IT-enabled collaboration in ways that allow broad research communities to have access to diverse data and to improve the conduct of science and engineering now and in the future to revitalize U.S. leadership in R&D
  - **Integrated multidisciplinary research**: Support research, development, and education that address societal challenges using a 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
  - **Humans in the loop**: Advance our understanding of the complex and increasingly coupled relationships between people and computing, with an emphasis on IT designed to fit the needs of its users, and enable explorations of creative ideas, novel theories, and innovative technologies that promise to transform the way humans communicate, work, learn, play, and maintain their health

- **IT and education**
  - **Transform science teaching across educational settings**: Integrate 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 education settings to enhance learning anytime in any location, and provide learning personalized and tailored to the needs of diverse learners; and 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 and computer security
  - **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

Highlights of the Request

The SEW agencies report the following topical areas as highlights of their planned R&D investments for FY 2014. Agencies are listed in alphabetical order:

- **Understand and support collaboration**
  - **Multidisciplinary centers, institutes, and communities**: Support collaborative activities to advance a field or create new directions in research or education by enabling 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
  - **Human-centered computing**: 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
  - **Improving health and wellbeing**: Leverage the scientific methods and knowledge bases of a broad range of computing and communication research perspectives to facilitate long-term, transformative change in how we treat illness and maintain our health; improve safe, effective, efficient, equitable, and patient-centered health and wellness services – NIH and NSF
  - **Sustainability science, engineering, and education**: Generate the discoveries and capabilities in climate and energy science and engineering needed to inform societal actions that lead to environmental and economic sustainability; support interdisciplinary communities focused on sustainability science – NSF
- **IT and 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 more 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, NSF and ONR

- **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 – DHS, DoD, NIST, and other agencies

Planning and Coordination Supporting Request

The SEW-Collaboration team (SEW-Collab) plans to engage in a series of workshop discussions over the coming year to develop a SEW-Collab strategic plan and associated agenda. The SEW-Education team (SEW-Ed) continues to pursue opportunities for expanded interagency collaborations to address ways of improving IT education and workforce training. Preliminary steps included outreach to non-NITRD agencies and workshop discussions on possible elements of the SEW-Ed agenda. SEW also promotes interactions between IT researchers, practitioners, and government policymakers. Current activities include:

- **Articulate program and priority similarities across agencies**: Develop coordination plans for sharing robust practices; identify gaps and develop plans to prioritize and address them; incorporate input from a broad cross section of stakeholders; and prepare a comprehensive strategic plan document – SEW agencies and others

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 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 Strategic Plan; assess and leverage DoD STEM investments
- **DOE/NNSA**: Critical-skills development program for university participants in the Advanced Simulation and Computing (ASC) Alliance Program
- **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; Transformative Computational Science using CyberInstrastructure (CI TraCS) effort to support outstanding scientists and engineers who have recently completed doctoral studies and are interested in pursuing postdoctoral activities in computational science; 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 (DR K-12) program for significant and

sustainable improvements in STEM learning, advance STEM teaching, and contribute to improvements in the Nation's formal education system

- **ONR**: The Information Dominance and Cybersecurity program seeks to advance the science of security through interdisciplinary research to ensure safe and secure operations in cyberspace; the Naval Research Enterprise Summer Intern Program (NREIP) allows students to participate in naval research; Mission Ocean allows fifth-through eighth-grade level students to gain hands-on experience operating a simulated submarine; and the SeaPerch Program provides students with the opportunity to learn about robotics, engineering, science, and mathematics while building an underwater remotely operated vehicle (ROV) as part of a science and engineering curriculum; Technovation Challenge allows high school-aged entrepreneurial young women to pair with a female near-peer mentor for a team App development competition working with venture capitalists who develop and release the winning App; National Junior Science and Humanities Symposia (JSHS) jointly funded by Army, Navy, and Air Force to promote original research and experimentation in science, engineering, and mathematics at the high school level

Software Design and Productivity (SDP)

NITRD Agencies: AFOSR, AFRL, DARPA, DHS, NASA, NIH, NIST, NOAA, NSF, ONR, and OSD

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 use computational machinery. Pervasive computational behaviors present enormous opportunities for industry and society but also pose significant challenges. These challenges require 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 2014 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 cross-cutting 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 2014. 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; 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, DARPA, 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 – FAA and NASA
- **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, 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 (NCAR)
- **Automatic program and processor synthesis for data dependent applications:** From high-level mathematical description, generate code with performance comparable to hand-written code – ONR
- **Next-generation aircraft**: Collaboration on concepts, modeling and simulation tools – DoD Service research organizations, FAA, and NASA

Additional 2013 and 2014 Activities by Agency

The following list provides a summary of individual agencies' ongoing programmatic interests for 2013 and 2014 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 framework (MDAO) 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; Units Markup Language; precisely and accurately define classes of software weaknesses which will serve as a basis for tool interoperability and proofs that a tool or technique precludes certain classes of weaknesses; run SATE to understand the contribution of such tools to assurance; and 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 Earth System Modeling Framework (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**: Technologies for real-time control of distributed and embedded systems; methods for intelligent orchestration of Web services; language and system for building secure, federated, distributed information systems; analysis tools for modeling, testing software component interactions; software for quantum processing; automate software de-bloating and de-layering to reduce software complexity, size/attack-surface, and achieve highly efficient, compact, secure programs; develop novel architectures and protocols

for real-time control of embedded sensors, develop new reference architectures for embedded systems, and promote reusability

- **OSD**: SDP research as a critical part of the overall DoD software assurance posture. OSD's primary effort in SDP is in the research program at the Software Engineering Institute Federally Funded Research and Development Center. The program addresses composability and timing at all scales, computing for real-time and embedded systems, multicore programming, computing at the tactical edge, and system of system architectures. The OSD Software Producibility Initiative addresses tools and techniques to improve the efficiency of software production across the DoD. The initiative includes correct-by-construction methods, model-driven development, validation and verification of complex systems (greater than 20 million lines of code), software visualization, static and dynamic analysis, deterministic behavior in software, interoperable multiscale and multidomain models, and efficient execution of distributed and multicore processing. Additional OSD programs, such as the Joint Capability Technology Demonstration (JCTD), also address SDP. JCTD is a collection of efforts to apply advanced technology development to a broad set of current military challenges. Among those efforts is software development to combine sensor data from disparate sources.

Additional Program Focus Areas

Big Data R&D (BD R&D)

Participating Agencies: DARPA, DoD Service Research Organizations, DOE/NNSA, DOE/SC, EPA, 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 between agencies, academia, and the private sector; and identify the goals for a National Big Data R&D Initiative. As data volumes grow exponentially, so does the concern regarding data preservation, access, dissemination, and usability. Research in areas such as database interoperability, machine learning, automated analysis, visualization, and improved data privacy and security will help advance science and inspire revolutionary research techniques.

Strategic Priorities

The BD SSG envisions a future in which the ability to analyze and extract information from large, diverse, and disparate data sets accelerates the process of scientific discovery and innovation; promotes new economic growth; and leads to new fields of research and new areas of inquiry that would otherwise be impossible. The BD SSG strategic priorities include:

- Core technologies
- Big data infrastructure
- Workforce development
- Competitions and challenges

Current and Planned Coordination Activities

The current and planned coordination activities of the BD SSG include:

- In March 2012, the White House Office of Science and Technology Policy launched the National Big Data R&D Initiative.[11] Six agencies – NSF, NIH, DoD, DARPA, DOE, and USGS – announced new big data projects at the launch event, including the joint NSF-NIH solicitation, *Core Techniques and Technologies for Advancing Big Data Science & Engineering*. The *Fact Sheet: Big Data Across the Federal Government*[12], released at the event, included a compilation of information provided by the BD SSG on over 65 federal projects.
- The joint NSF-NIH Solicitation, *Core Techniques and Technologies for Advancing Big Data Science & Engineering*, developed under the aegis of the BD SSG, is intended to "advance the core scientific and technological means of managing, analyzing, visualizing, and extracting useful information" from big data, particularly those technologies that are relevant across multiple agency missions. The solicitation generated great interest and resulted in several hundred high quality proposals. In addition to the mid-scale projects awarded in Fall 2012, small project awards are to be announced in Spring 2013.
- To help ensure a trained workforce to capitalize on big data resources, the BD SSG created an inventory of the workforce development programs at nine agencies. [13] The group plans to use this information, combined with information gathered from academia and the private sector, to develop recommendations on how to develop an effective big data workforce.

[11] http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf
[12] http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_fact_sheet_final.pdf
[13] Census, CIA, DHS, DoD, DOE, ED, NIH, NSA, NSF

- To explore the use of challenges and competitions, NSF, NASA, and DOE/SC jointly launched a series of Big Data Challenges beginning in October 2012. Receipt of submissions, judging, and awards started in November 2012 on a rolling basis. This series of challenges is designed not only to identify unique applications for the use of multiagency big datasets, but also as a way to identify the core technology that is needed to turn heterogeneous data into more homogeneous, interoperable data. The series is expected to continue throughout 2013.[14]
- The BD SSG is examining big data infrastructure development for domain science (also known as domain research projects). The group identified four existing federal projects[15] that involve big data and are, or could become, relevant to multiple agencies. Over the upcoming year, activities include exploring each project through interviews and joint meetings to determine the infrastructure needed to realize the full potential of currently available data or future data. The group plans to synthesize and use the information to develop recommendations for big data infrastructure.
- A second National Big Data R&D Initiative event is planned for 2013 to bring together federal, academic, and private sector stakeholders to discuss progress made and identify areas for investment.

[14] http://community.topcoder.com/coeci/nitrd
[15] Climate Change and Public Health; Materials Genome Initiative; Space Weather; Electronic Health Records

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, to address the need for streamlined decision processes and dynamic responsiveness to changing 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 research and development coordination activities. The CSIA R&D SSG's strategic priorities include:

- Prioritizing federal cybersecurity research and development areas and ensuring that the entire spectrum of research and development priorities and key technology challenges across the Federal Government are being addressed
- Leading strategic research and development coordination efforts in addressing the Administration priorities (such as the President's Cyberspace Policy Review)
- Formulating and evolving a framework for research and development strategies that focuses on game-changing technologies

Current and Planned Coordination Activities

The CSIA R&D SSG planned activities include:

- Coordinating strategic research and development objectives and the allocation of federal budgets to support them
- 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 research and development 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
- Cultivating and supporting a research community in the area of the science of security
- Developing focused activities to help accelerate the transition of research into practice
- Coordinating and promoting activities leading to effective education programs and career options in cybersecurity

Health Information Technology R&D (HITR&D)

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

The Health Information Technology R&D Senior Steering Group (HITR&D 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 research and development programs related to health information technology.

The HITR&D SSG established the Health Information Technology Innovation and Development Environments (HITIDE) Subgroup. The aim of the HITIDE Subgroup is to advance the development of interoperable health IT systems by leveraging the existing testbed environments of federal agency health IT systems for a virtual test, development, and innovation ecosystem.

Participants in the HITR&D SSG and HITIDE Subgroup 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 HITR&D SSG 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 HITR&D SSG include:

- Addressing multiagency leadership in health IT interoperability and the development of innovative applications
- Bringing together the health IT and information technology R&D communities to focus on health IT research and development needs

Current and Planned Coordination Activities

The current and planned coordination activities of the HITR&D SSG include:

- *Research Gaps*: Analyzing IT R&D gaps related to electronic health records, evidence-based decision support, standards and interoperability, privacy and security, modeling and simulation, data analytics, natural language processing, semantic technologies, knowledge repositories and metadata usage, public health surveillance, patient safety, clinical quality measures, clinical trials, personalized 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
- *Federated Testbeds*: Developing a HITIDE Memorandum of Understanding and governance entities to facilitate cooperation among multiple federal agencies with interests in leveraging the existing testbed environments of federal agencies' health IT systems to advance research, innovation, and interoperable health IT systems
- *Health IT R&D Needs*: Assessing health IT research and development needs against the shifting landscape of today's healthcare system and the profound transformation that the system is undergoing due, in part, to widespread adoption of health IT, changes in care payment models, the influx of consumer and business intelligence IT to healthcare settings (for example, mobile devices, social computing, and big data analytics), and major scientific breakthroughs in understanding the role of the genome in health and disease

Wireless Spectrum R&D (WSR&D)

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

The Wireless Spectrum R&D Senior Steering Group (WSR&D SSG) was established in 2010 in response to the June 28, 2010 *Presidential Memorandum – Unleashing the Wireless Broadband Revolution*.[16] The memorandum calls for NITRD to assist the Secretary of Commerce in creating and implementing a plan to facilitate research, development, experimentation, and testing by researchers to explore innovative spectrum-sharing technologies.

Strategic Priorities

WSR&D SSG member agencies have been funding research and development techniques that enable more efficient use of the radio spectrum through spectrum-sharing technologies. Working within the requirements of the Presidential Memorandum and with guidance from the President's Chief Technology Officer, the WSR&D SSG has held several workshops to gather information from academic and private sector researchers to help maximize the group's R&D efforts to increase the use of spectrum sharing in both the government and the private sectors. The WSR&D SSG continues to be guided by the following strategic objectives:

- *Transparency*: Communicate to both federal agencies and the private sector the research and development 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 research and development 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 WSR&D SSG is developing a series of reports based upon findings gathered from monthly informational meetings and public-private workshops. The following summary highlights the SSG's activities and plans:

- The WSR&D SSG created an inventory by collecting information on approximately 600 federal R&D projects in the spectrum-sharing domain. The inventory report, *Federal Spectrum Sharing Research Inventory*, is available on the NITRD website and updated periodically. The inventory served as the basis of the first WSR&D SSG workshop, held July 2011 in Boulder, Colorado, in which the academic and private sector communities engaged in a dialog about the portfolio of research projects. *Toward Innovative Spectrum Sharing Technologies*, the workshop report publicly released in November 2011, reflects the recommendations and conclusions from the workshop regarding general priority research areas.
- Based on a second workshop held in January 2012, the WSR&D SSG delivered to OSTP a second workshop report, *Examining the Need for a National Spectrum Sharing Testing Environment*. This report, publicly released in September 2012, summarized the group's findings and provided recommendations for the development of a national level spectrum-sharing test facility coordination effort. These recommendations are being taken into account in current discussions about a potential coordinated national testbed capability. In addition, the WSR&D SSG created a unique online testbed information portal[17] that integrates with Google Maps©. The portal shows the locations and capabilities of existing federal testbed facilities, and indicates the status and availability of each facility to academic and private sector researchers.

[16] http://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution, Section 3.
[17] http://www.nitrd.gov/Subcommittee/wsrd/Testbeds/map.aspx

- A third workshop, held in July 2012, focused on collecting and exploring actual projects targeted to remove persistent barriers to spectrum-sharing adoption. In advance of the workshop, researchers submitted outlines of proposed research to help facilitate Executive, Congressional, and Agency mandates and goals in this area. At the workshop, the group of researchers, drawn from academia, the private sector, and the Federal Government, presented, discussed, and prioritized the proposals. This effort resulted in recommendations that the SSG delivered to OSTP in November 2012 in the workshop report *Research Proposals that Facilitate Spectrum Sharing Adoption*. Among other potential uses, NSF plans to use the recommendations to inform priority investment areas for its FY 2013 Enhancing Access to the Radio Spectrum (EARS) program.
- A fourth workshop, held in April 2013, focused on the larger spectrum-sharing ecosystem and examined the barriers to adoption from an economic and social incentive/disincentive perspective. The SSG identified these barriers as important to overcome, not only for the adoption of spectrum-sharing technologies, but also for technology transfer between the Federal Government and the private sector. The group's consensus is that further research in these areas is warranted and it plans to prepare recommendations accordingly.
- A workshop to examine privacy and security issues surrounding spectrum sharing is under consideration for late 2013 to help inform recommendations in this area.

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

Participating Agencies: DARPA, DoD Service Research Organizations, DOE/SC, DHS, NARA, NASA, NIH, NIST, NOAA, OSD, and VA

The Federal 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
- Ontology technology
- Wikis and open collaboration
- EarthCube
- Emerging technologies
- Sharing knowledge, ideas, and best practices

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 Expedition and Emerging Technology workshops as well as monthly meetings with invited guest speakers to achieve this goal, including:

- *Cloud computing*: FASTER encourages collaboration with NIST and NOAA cloud computing activities by using the U.S. Government Cloud Computing Technology Roadmap to develop the NIST Cloud Computing Standards & Technology Roadmap and give focus to interoperability, portability, and security
- *Ontology technology*: FASTER members participated in the Ontology Summit of 2012, co-chaired the Ontology and Big Data Challenge session, and contributed to the "Ontology for Big Systems: The Ontology Summit 2012 Communiqué"
- *Wikis and open collaboration*: encourages the use of wikis to make research and technology information available across agencies
- *EarthCube*: promotes participation in the EarthCube community. EarthCube is the novel approach taken by NSF to promote a series of ongoing engagements between multiple earth-centered science(s) communities and relevant technologists. Participants include cyberinfrastructure developers, institutions, and interested agencies that are contributing to an integrated infrastructure to transform the conduct of research within the geosciences

- *Emerging technologies*: FASTER attempts to bridge research and practitioner communities through dissemination of research technology information and operational requirements
- *Sharing knowledge, ideas and best practices*: FASTER plans to broaden its coordination efforts by addressing ways to improve the consumerization of IT and exploit innovative ways to advance the explosion of mobile applications that will serve to expedite the translation of research results. Currently it is exploring the use of challenges rewarded by prizes to bring the public and government together to solve problems

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
Helen D. Gill, NSF
William Bradley Martin, NSA
Albert J. Wavering, NIST

High End Computing (HEC) Interagency Working Group
*Co-Chairs**
John E. West, HPCMP
Lucy Nowell, DOE/SC

Human-Computer Interaction and Information Management (HCI&IM) Coordinating Group
Co-Chairs
Leslie A. Collica, NIST
Sylvia Spengler, NSF

Large Scale Networking (LSN) Coordinating Group
Co-Chairs
Robert J. Bonneau, AFOSR
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
Dan S. Katz, NSF
Richard Carlson, DOE/SC

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

SEW Teams:
SEW-Collaboration Team
*Chair***
Kevin Crowston, NSF

SEW-Education Team
Co-Chairs
Arlene de Strulle, NSF
Ernest McDuffie, NIST

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

Senior Steering Group, Subgroup, and Community of Practice Chairs

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

BD Subgroups:
Core Technologies
Co-Chairs
Tandy Warnaw, NSF
C. Suzanne Iacono, NSF
Infrastructure
Co-Chairs
Mark Suskind, NSF
Robert Chadduck, NSF
Michael Little, NASA
Challenges
Co-Chairs
C. Suzanne Iacono, NSF
Fen Zhao, NSF
Workforce Development
Co-Chairs
Sylvia Spengler, NSF
Sastry Pantula, NSF

Cyber Physical Systems (CPS) Senior Steering Group
Co-Chairs
Sivaraj Shyam Sunder, NIST
Keith Marzullo, NSF

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

Health Information Technology R&D (HITR&D) Senior Steering Group
Co-Chairs
Douglas B. Fridsma, ONC
Donald A.B. Lindberg, NIH
Howard D. Wactlar, NSF
George O. Strawn, NCO

HITR&D Subgroup:
Health Information Technology Innovation and Development Environments (HITIDE) Subgroup
*Co-Chairs****
Mark Goodge, DoD/MHS
Vacant

Wireless Spectrum R&D (WSR&D) Senior Steering Group
Co-Chairs
Byron Barker, NTIA
Andrew Clegg, NSF
Mark A. Luker, NCO

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

*Bryan Biegel, NASA, was Co-Chair of the HEC IWG through February 2013

**Susan Winter, formerly with NSF, was Co-Chair of the SEW CG and SEW-Collaboration Team through early January 2013

***Douglas E. Rosendale, formerly with VA, was Co-Chair of the HITIDE Subgroup through December 2012

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
ANI – Advanced Networking Initiative
ANL – DOE's Argonne National Laboratory
ARL – Army Research Laboratory
ARO – Army Research Office
ARSC – Arctic Region Supercomputing Center
ASC – DOE/NNSA's Advanced Simulation and Computing program
ASCR – DOE/SC's Advanced Scientific Computing Research
ASPR – Office of the Assistant Secretary for Preparedness and Response
ATC – Air traffic control
ATP – App Testing Portal
BD – Big Data, one of NITRD's Senior Steering Groups
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
C3I – Communications, Command, Control, and Intelligence
CBIIT – NIH's Center for Biomedical Informatics and Information Technology
CCF – Computing and Communication Foundations
CC-NIE – NSF's Campus Cyberinfrastructure-Network Infrastructure and Engineering
CDC – Centers for Disease Control and Prevention
CEMMSS – Cyber-enabled Manufacturing, Materials, and Smart Systems
CERDEC – U.S. Army's Communications-Electronics Research, Development, and Engineering Center
CG – Coordinating Group
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 activity
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
CoP – Community of Practice
COTs – Commercial off-the-shelf technologies
CPS – Cyber-physical systems
CRASH – Clean-slate design of Resilient, Adaptive, Secure Hosts
CRUSHPROOF – Cyber Unification of Security Hardening and Protection of Operational Frameworks
CSIA – Cybersecurity and Information Assurance, one of NITRD's eight Program Component Areas
DARPA – Defense Advanced Research Projects Agency
DECIDE – Distributed Environment for Critical Infrastructure Decision-making Exercises
DEFIANT – Defensive Enhancements for Information Assurance Technologies
DETER – NSF- and DHS-initiated cyber Defense Technology Experimental Research testbed

DeVenCI – Defense Venture Catalyst Initiative
DHS – Department of Homeland Security
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/INL – DOE's Idaho National Laboratory
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
E2E – End-to-End
EARS – Enhancing Access to the Radio Spectrum Program
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
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
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
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
HITR&D – Health Information Technology Research and Development, one of NITRD's Senior Steering Groups
HITIDE – HITR&D SSG's Health Information Technology Innovation and Development Environments Subgroup
HOST – Homeland Open Security Technology
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
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
JPDO – Joint Planning and Development Office
K-12 – Kindergarten through 12th grade
LANL – DOE's Los Alamos 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
MAGIC – LSN's Middleware and Grid Interagency Coordination team, previously named the Middleware and Grid Infrastructure Coordination team
MIC – Many integrated cores
MDAO – Multidisciplinary analysis optimization
Morphinator – Morphing Network Assets to Restrict Adversarial Reconnaissance
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
NCCS – NASA Center for Climate Simulation
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
NICE – National Initiative for Cybersecurity Education
NIH – National Institutes of Health
NIJ – DOJ's National Institute for 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/OCI – NSF's Office of Cyberinfrastructure
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
N-Wave – NOAA's high speed network
ODNI – Office of the Director of National Intelligence
OFR – Treasury's Office of Financial Research
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
R&D – Research and development
RDT&E – DoD's Research Development Test & Evaluation programs
ROV – Remotely operated vehicle
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
SATE – NIST's Software 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
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
SHARP – ONC's Strategic Health IT Advanced Research Projects
SI^2 – NSF's Software Infrastructure for Sustained Innovation
SNL – Sandia National Laboratories
SSG – Senior Steering Group
State – Department of State
STEM – Science, technology, engineering, and mathematics
STONESOUP – IARPA's Security Taking on New Executable Software of Uncertain Provenance activity
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
TIS – NSF's XD Technology Insertion Service program
Treasury – Department of the Treasury
TwC – NSF's Trustworthy Computing program
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
VA – Department of Veterans Affairs
V&V – Verification and validation
VOSS – NSF's Virtual Organizations as Sociotechnical Systems program
VSTTE – Verified software, theories, tools, and experiments
WAIL – NSF's Wisconsin Advanced Internet Laboratory
WAN – Wide area network
WSR&D – Wireless Spectrum Research and Development, one of NITRD's Senior Steering Groups
XD – NSF's eXtreme Digital program
XSEDE – 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

http://www.nitrd.gov