THE NETWORKING & INFORMATION TECHNOLOGY RESEARCH & DEVELOPMENT PROGRAM

SUPPLEMENT TO THE PRESIDENT'S FY2019 BUDGET

Product of the

SUBCOMMITTEE ON NETWORKING & INFORMATION TECHNOLOGY RESEARCH & DEVELOPMENT

COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

AUGUST 2018

About This Document

This document is a supplement to the President's FY2019 Budget Request to Congress. It describes activities planned for FY2019 by the Federal agencies participating in the Networking and Information Technology Research and Development (NITRD) Program. It reports actual investments for FY2017, estimated investments for FY2018, and requested funding levels for FY2019 by agency and Program Component Area (PCA). For the FY2019 budget request, this Supplement identifies the strategic priorities, key programs, and key coordination activities of each NITRD PCA. An appendix to the Supplement, *FY2019 Federal Cybersecurity R&D Strategic Plan Implementation Roadmap*, lists existing and proposed Federal R&D projects and programs that address the Nation's critical cybersecurity challenges; it is available at https://nitrd.gov/pubs/FY2019-Cybersecurity-RD-Roadmap.pdf.

About the National Science and Technology Council

The NITRD Program is managed by the NITRD Subcommittee of the National Science and Technology Council (NSTC) Committee on Science and Technology Enterprise. The NSTC is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at https://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at https://www.whitehouse.gov/ostp.

About the NITRD Program

The Networking and Information Technology Research and Development Program is the Nation's primary source of federally funded research and development (R&D) on networking and information technology (IT). The NITRD Program seeks to maximize interagency coordination in providing the R&D foundations for continued U.S. technological leadership and meeting the needs of the Federal Government for advanced IT. The Program also seeks to accelerate development and deployment of advanced IT to support American military superiority, security, economic prosperity, energy dominance, and health, while it supports innovation and early-stage research, modernization of the IT research infrastructure, and development of a strong cyber-enabled workforce. The NITRD Program—established by the High-Performance Computing Act of 1991 (P.L. 102-194) and reauthorized by Congress in the American Innovation and Competitiveness Act of 2017 (P.L. 114-329)—is one of the oldest and largest of the formal Federal programs that engage multiple agencies in coordination activities. More information is available at https://www.nitrd.gov.

About the NITRD National Coordination Office

The National Coordination Office (NCO) supports the NITRD Program, the NITRD Subcommittee, and its Interagency Working Groups (IWGs) by providing technical expertise, planning, and coordination, and by serving as the Program's central point of contact. The NCO continuously seeks to enhance its ability to be a catalyst for collaboration, exchange of information, and outreach to foster knowledge, methods, R&D, technology transfer, and innovation for U.S. global leadership in networking and information technology and its applications. In cooperation with NITRD agencies and IWGs, the NCO prepares and disseminates the annual NITRD Supplement to the President's Budget. More information is available at https://www.nitrd.gov/about/about-nco.aspx.

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.

National Science and Technology Council

Chair, Ted Wackler, Deputy Chief of Staff and Assistant Director, OSTP

Staff: Chloe Kontos, Executive Director, NSTC

Committee on Science and Technology Enterprise
Subcommittee on Networking and Information Technology Research and Development

Co-Chair, Kathleen (Kamie) Roberts (NCO)

Co-Chair, Erwin Gianchandani (NSF)

Executive Secretary, Nekeia Butler (NCO)

National Coordination Office for Networking and Information Technology Research and Development

Director, Kathleen (Kamie) Roberts

NITRD Subcommittee Members

Department of Commerce (DOC)

National Institute of Standards and Technology (NIST)
Representative
Charles H. Romine
Alternate
Elham Tabassi

National Oceanic and Atmospheric Administration (NOAA)
Representative
Frank Indiviglio
Alternate
Leslie Hart

Department of Defense (DoD)

Defense Advanced Research Projects Agency (DARPA)
Representative
Brian Pierce

Military Services

Air Force
Representative
Anthony M. Newton

Army
Representative
Thomas Russell
Alternate
Nora Pasion

Navy
Representative
Joan S. Cleveland
Alternate
Sukarno Mertoguno

National Security Agency (NSA)
Representative
George Coker

Office of the Secretary of Defense (OSD)
Representative
Richard Linderman
Alternate
Dai H. Kim

Department of Energy (DOE)

National Nuclear Security Administration (DOE/NNSA)
Representative
Mark Anderson
Alternate
Thuc T. Hoang

Office of Electricity Delivery and Energy Reliability (DOE/OE)
Representative
Carol Hawk

Office of Science (DOE/SC)
Representative
Barbara Helland
Alternate
Ceren Susut-Bennett

Department of Health and Human Services (HHS)

Agency for Healthcare Research and Quality (AHRQ)
Representative
Christine Dymek
Alternate
Chun-Ju (Janey) Hsiao

National Institutes of Health (NIH)
Representative
Susan Gregurick
Alternate
Peter Lyster

Office of the National Coordinator for Health Information Technology (ONC)
Representative
Teresa Zayas Cabán
Alternate
Kevin Chaney

Department of Homeland Security (DHS)

Representative
Douglas Maughan
Alternate
Scott W. Tousley

Department of Justice (DOJ)

National Institute of Justice (NIJ)
Representative
William Ford
Alternate
Mark Greene

Independent Agencies

Environmental Protection Agency (EPA)
Representative
Gary L. Walter

National Aeronautics and Space Administration (NASA)
Representative
Terry Jackson

National Archives and Records Administration (NARA)
Representative
Mark Conrad

National Reconnaissance Office (NRO)
Representative
Thomas Jenkins

National Science Foundation (NSF)
Representative
Erwin Gianchandani

Executive Office of the President

Office of Management and Budget (OMB)
Representative
Tali Bar-Shalom

Office of Science and Technology Policy (OSTP)
Representative
Lloyd J. Whitman

Other Participating Departments and Agencies

These Federal departments and agencies participate in NITRD activities and have mission interests in advanced networking and IT R&D and applications; they support NITRD Program coordination but do not participate in the NITRD Subcommittee.

Department of Agriculture (USDA)
- Agricultural Research Service (ARS)
- National Institute of Food and Agriculture (NIFA)

Department of Commerce (DOC)
- International Trade Administration (ITA)
- National Telecommunications and Information Administration (NTIA)
- United States Census Bureau (Census)

Department of Defense (DoD)
- Defense Information Systems Agency (DISA)
- DoD Intelligence Information Systems (DoDIIS)
- National Geospatial-Intelligence Agency (NGA)
- Special Operations Command (SOCOM)
- United States Marine Corps (USMC)

Department of Education (ED)

Department of Energy (DOE)
- Office of Cybersecurity, Energy Security, and Emergency Response (DOE/CESER)
- Office of Energy Efficiency and Renewable Energy (DOE/EERE)
- Office of Environmental Management (DOE/EM)

Department of Health and Human Services (HHS)
- Centers for Disease Control and Prevention (CDC)
- Food and Drug Administration (FDA)
- Health Resources and Services Administration (HRSA)
- National Institute for Occupational Safety and Health (NIOSH)
- National Institute on Disability, Independent Living, and Rehabilitation Research (NIDILRR)

Department of Housing and Urban Development (HUD)

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

Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- Drug Enforcement Administration (DEA)

Department of Labor (DOL)
- Bureau of Labor Statistics (BLS)
- Occupational Safety and Health Administration (OSHA)

Department of State (DOS)

Department of Transportation (DOT)
- Federal Aviation Administration (FAA)
- Federal Highway Administration (FHWA)
- Intelligent Transportation Systems Joint Program Office (ITS JPO)

Department of the Treasury (Treasury)

Department of Veterans Affairs (VA)

Federal Communications Commission (FCC)

Federal Deposit Insurance Corporation (FDIC)

Federal Trade Commission (FTC)

General Services Administration (GSA)

Nuclear Regulatory Commission (NRC)

Office of the Director of National Intelligence (ODNI)
- Intelligence Advanced Research Projects Activity (IARPA)
- National Counterintelligence and Security Center (NCSC)
- National Counterterrorism Center (NCTC)

United States Agency for International Development (USAID)

United States Office of Personnel Management (OPM)

United States Postal Service (USPS)

Table of Contents

1. Introduction and Overview

Information technology (IT) is perhaps the most broadly transformative technology ever invented, with impacts on defense, security, energy, healthcare, and more. Innovation in IT continually enables pivotal new applications that advance U.S. national priorities and Federal agency missions. For 27 years, the Networking and Information Technology Research and Development (NITRD) Program has been the Nation's primary source of federally funded research and development (R&D) on networking and information technology. The Program maximizes coordination of Federal IT R&D to optimize Federal investments that support agency missions and contribute to the public good.

The NITRD Program is tasked with providing the IT R&D foundations for assuring continued U.S. leadership in science and technology, supporting investments that develop tools and technologies with the potential to open new areas of discovery, and increasing government accountability and efficiency with advanced IT. The NITRD Program provides a framework and mechanisms to maximize coordination among the many Federal agencies that support R&D in advanced information technologies and report IT research budgets in this NITRD Supplement to the President's fiscal year (FY) 2019 Budget. As required by legislation, this NITRD Supplement details the NITRD Program's FY2019 requested budgets by participating agency and Program Component Area (PCA) to meet Program goals and national priorities for state-of-the-art IT and software R&D.

The NITRD Program was established by the High-Performance Computing Act of 1991 (P.L. 102-194) and reauthorized three times, most recently in 2017 by the American Innovation and Competitiveness Act (P.L. 114-329).[1] It is managed by the NITRD Subcommittee of the National Science and Technology Council's (NSTC) Committee on Science and Technology Enterprise and supported by the NITRD National Coordination Office (NCO). In addition to the 21 agencies that are formal NITRD members, over 40 other agencies with IT interests also participate in NITRD strategic planning, information sharing, and collaborative activities as a means to contribute to and leverage the important technological advances arising from Federal networking and information technology R&D efforts.[2]

Advancing National R&D Priorities

Technologies developed from NITRD Program research activities continue to improve the lives of all Americans. The following examples, distilled from this NITRD Supplement, illustrate how the Federal IT and networking R&D coordinated by the NITRD Program advance national priorities, as described in the FY2019 Administration R&D Budget Priorities memorandum.[3]

Federal R&D in high-capability computing is advancing state-of-the-art, dual-use technologies and tools to defeat emerging threats on the physical and cyber battlefields, including applications ranging from military platform analysis to artificial intelligence; supporting exascale and quantum computing that accelerate innovation and will shorten time to market; and paving the way to modernizing and effectively managing research infrastructure, including leading-edge supercomputing facilities.

---

[1] Sec. 105 of Public Law 114-329 is the "Networking and Information Technology Research and Development Modernization Act of 2016"; https://congress.gov/bill/114th-congress/senate-bill/3084/text#toc-idB56FB943F79348E9AEE03036E5C90675.

[2] Pages iii and iv list member and nonmember departments and agencies that participate in NITRD program activities.

[3] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-30.pdf

Cybersecurity R&D is developing capabilities to provide the U.S. military an advantage by developing effective cyber-defensive technologies and improved cyber-situational awareness. Participating agencies are also strengthening national security by developing cybersecurity capabilities that improve the resiliency of cyber and cyber-physical systems, protect national assets against cyber attacks, enable the Nation's critical infrastructure to withstand cyber incidents, and allow for timely and appropriate cyber responses.

Federal intelligent robotics and autonomous systems R&D enables teams of autonomous vehicles for disaster response and first responder safety, intelligent and collaborative robots that strengthen U.S. manufacturing competitiveness, and intelligent robotics to enhance surgery and support independent living.

Agencies active in networking technology R&D are developing, standardizing, and deploying technologies that enhance infrastructure security, protect end-to-end communications, provide networking support, provide control and situational awareness capabilities, support cyber defense at scale, and enable future networked information systems.

Federal R&D in computing-enabled networked physical systems is helping the Nation realize the smart electric grid of the future by enabling development of real-time, adaptive, and interoperable electric grid cyber-physical systems that increase grid reliability, resilience, and security.

Other NITRD Program R&D and coordination activities include work to provide trust and resilience in software that enables it to recover from attacks in real time; innovation in reusable community-based big data analytics tools and open datasets that promote the fusion of ideas to address grand-challenge problems in science and society; video analytics such as face-in-video recognition for law-enforcement and anti-terrorism operations; medical device interoperability to enable safer and data-informed medical care; innovative interfaces for people to interact with energy systems to support more efficient and effective use of energy; privacy-enhancing technologies for securely sharing personal health data; and spectrum-sharing capabilities and spectrum-maneuverable communications for battlefield applications.

All NITRD agencies are focused on developing a future-focused workforce through a variety of programs, including partnerships that expand computer science, math, and engineering education at all grade levels, and activities that are building a robust ecosystem of cybersecurity education, training, and workforce development to ensure sufficient talent to meet growing IT security threats.

Highlights of the NITRD Program can be found at https://www.nitrd.gov/about/nitrd-highlights.aspx.

Budget Reporting Structure

The NITRD budget reporting structure is organized by Program Component Area and by agency to facilitate budgetary and programmatic comparisons from year to year. The PCAs are the major subject areas under which the interagency projects and activities coordinated through the NITRD Program are grouped.

Program Component Areas

There are ten NITRD PCAs, as listed below. The scopes (i.e., technical content) of the ten NITRD PCAs are the same in this FY2019 Supplement as in the FY2018 Supplement, although the definitions of all PCAs have been streamlined for consistency and concision. The names of three NITRD PCAs have been updated from the FY2018 PCAs, as indicated in the list below and depicted in Figure 1.

- Computing-Enabled Human Interaction, Communications, and Augmentation (CHuman)
- Computing-Enabled Networked Physical Systems (CNPS)
- Cyber Security and Privacy (CSP) (*formerly Cyber Security and Information Assurance [CSIA]*)
- Education and Workforce (EdW)
- Enabling R&D for High-Capability Computing Systems (EHCS)
- High-Capability Computing Infrastructure and Applications (HCIA)
- Intelligent Robotics and Autonomous Systems (IRAS) (*formerly Robotics and Intelligent Systems [RIS]*)
- Large Scale Data Management and Analysis (LSDMA)
- Large Scale Networking (LSN)
- Software Productivity, Sustainability, and Quality (SPSQ) (*formerly Software Design and Productivity [SDP]*)

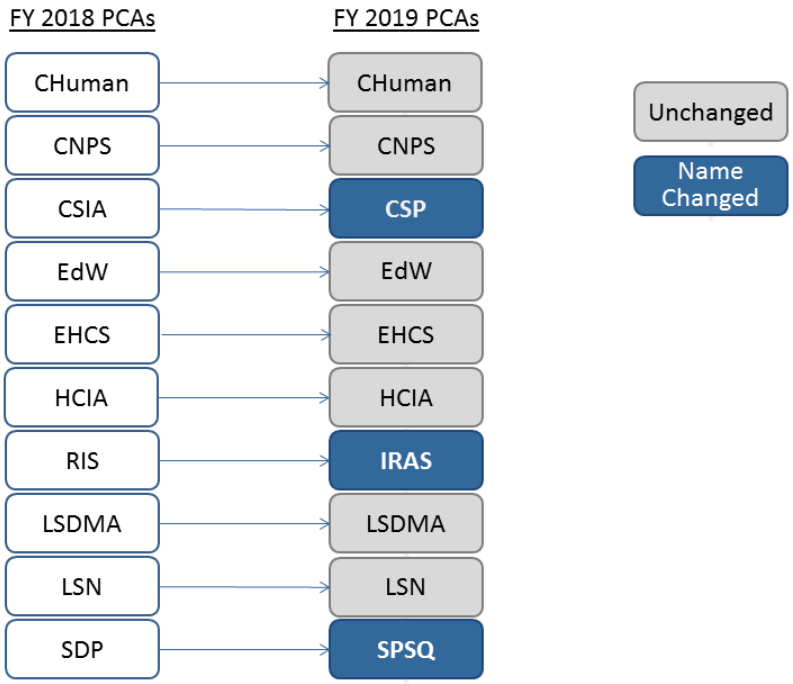


Figure 1. Relationships between the NITRD PCAs in FYs 2018 and 2019.

Interagency Working Groups

Federal agencies whose missions require ongoing IT R&D coordinate that work through one or more of NITRD's 13 Interagency Working Groups to achieve the best value from their R&D investments in the PCAs. With legislative guidance and with support from the NITRD NCO, the IWGs work in the following ways to coordinate R&D investments, increase government efficiency, yield greater R&D impact, and build community consensus and engagement:

- Maximize coordination of high-impact Federal R&D and research infrastructure by aligning with Administration and agency priorities, optimizing interagency coordination and collaboration, preparing and implementing action plans and roadmaps as needed, and conducting interdisciplinary coordination.

- Enable group productivity by maintaining a forward-looking work plan, conducting regular coordination meetings, selecting co-chairs as needed, seeking broad and engaged membership, publishing group products in a timely manner, and routinely seeking agency and member feedback.
- Engage effectively with NITRD stakeholders, including supporting interactions with Federal stakeholders, organizing constructive outreach activities with non-Federal stakeholders, and supporting workforce development.

Structure of this Supplement

Section 2 provides budget data for R&D investments made in FY2017, underway in FY2018, and requested in the President's FY2019 Budget in the ten NITRD PCAs, along with analyses that highlight key aspects of the NITRD investments. Section 3 contains subsections for each PCA that describe planned FY2019 Federal R&D activities associated with the funding presented in Section 2, as coordinated by one or more NITRD IWGs. Section 4 briefly reviews several NITRD interagency coordination activities that do not currently fall within any NITRD PCA. Appendix A defines the abbreviations used in this document.

2. NITRD Budgets by Agency and PCA, FYs 2017–2019

This section presents the NITRD budget by agency and PCA, including FY2017 actuals, FY2018 estimate, and the FY2019 request. An analysis of the significant changes between the FY2018 estimate and FY2019 request provides insight into trends in the NITRD agencies' budget allocations across the ten NITRD PCAs.[4] Additional information on NITRD-related R&D expenditures from FY2000 to FY2019 may be found at https://www.nitrd.gov/apps/itdashboard/.

Overview

The President's 2019 budget request for the NITRD Program is $5.28 billion, as depicted in Charts 1 and 2 and Table 1 below. This is an increase of approximately 2.52 percent, or $0.13 billion, compared to the $5.15 billion estimate in 2018. The overall change is due to both increases and decreases in individual agency NITRD budgets, which are described in the budget analysis section that follows Table 1.

Budget Charts

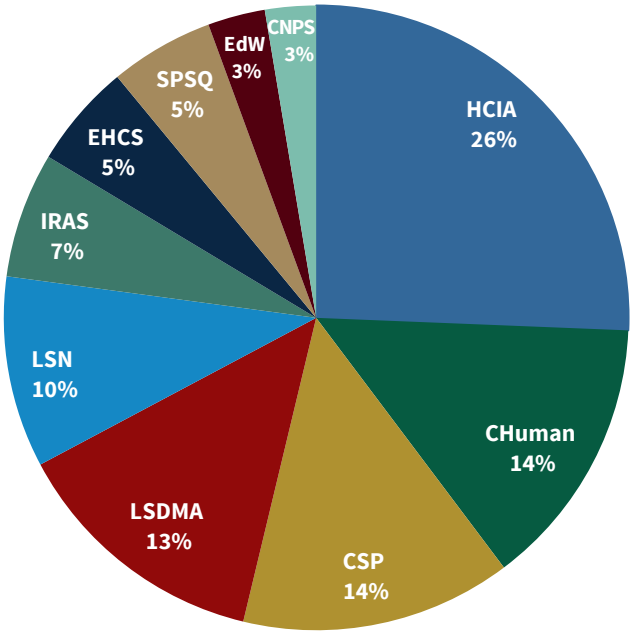
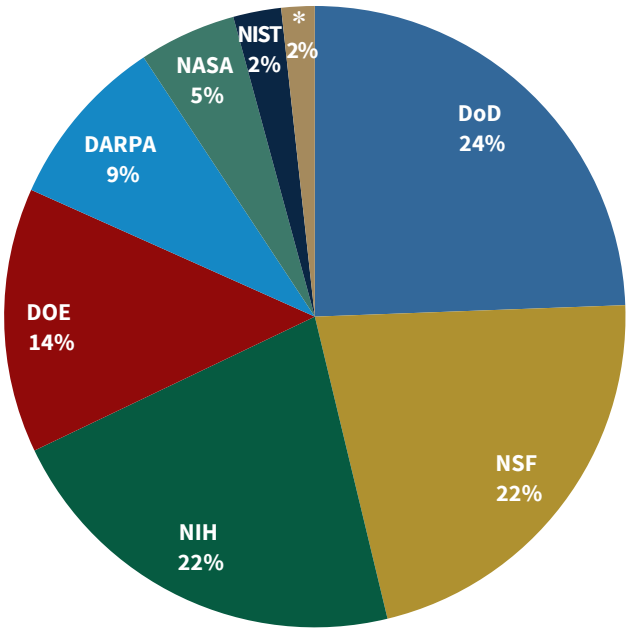


Chart 1. FY2019 Budget Request, as percentages of the total NITRD request, by PCA.



***Other:** AHRQ, DHS, DOT, EPA, NARA, NIJ, DOE/NNSA, and NOAA

Chart 2. FY2019 Budget Request, as percentages of the total NITRD request, by agency.

[4] FY2018 appropriated budgets were not available at the time this document was prepared; FY2018 estimates are based on annualized FY2018 continuing resolution levels.

Table 1. Agency NITRD Budgets by PCA, FYs 2017–2019

FY2017 Budget Actuals, FY2018 Budget Estimates,[a] and FY2019 Budget Request (Dollars in Millions)

Agencies are listed in order by FY2019 Budget Request, highest to lowest. The notes key is on the next page.

Agency	Budget Year	10 NITRD Program Component Areas										Total[b]
		CHuman	CNPS	CSP	EdW	EHCS	HCIA	IRAS	LSDMA	LSN	SPSQ	
DoD[c]	FY2017 Actual	169.0	19.6	176.8	19.9	52.6	308.5	117.4	95.1	148.0	13.1	1,120.1
	FY2018 Estimate	*168.4*	*24.3*	*211.0*	*15.0*	*44.2*	*278.4*	*124.8*	*117.3*	*177.7*	*22.4*	*1,183.4*
	FY2019 Request	**178.4**	**22.1**	**213.1**	**12.6**	**47.9**	**287.6**	**157.0**	**156.6**	**186.6**	**26.4**	**1,288.3**
NSF	FY2017 Actual	91.8	76.1	111.0	78.4	139.1	176.9	48.3	237.7	137.7	86.2	1,183.1
	FY2018 Estimate	*91.8*	*76.1*	*111.0*	*78.4*	*139.1*	*176.9*	*48.3*	*237.7*	*137.7*	*86.2*	*1,183.1*
	FY2019 Request	**86.1**	**82.3**	**106.4**	**78.3**	**121.7**	**190.9**	**41.8**	**237.0**	**130.3**	**77.3**	**1,152.0**
NIH	FY2017 Actual	410.1	23.1	4.7	52.1	28.6	228.4	6.9	228.1	12.8	170.8	1,165.5
	FY2018 Estimate	*400.8*	*23.0*	*4.3*	*49.9*	*28.6*	*227.4*	*6.9*	*224.3*	*12.5*	*169.0*	*1,146.7*
	FY2019 Request	**402.6**	**22.9**	**4.8**	**51.6**	**28.1**	**224.0**	**6.7**	**223.5**	**12.5**	**166.9**	**1,143.6**
DOE[d]	FY2017 Actual	0.0	0.0	39.5	10.0	43.7	389.7	0.0	0.0	60.1	0.0	543.0
	FY2018 Estimate	*0.0*	*0.0*	*40.7*	*10.0*	*44.3*	*396.3*	*0.0*	*0.0*	*70.9*	*0.0*	*562.3*
	FY2019 Request	**0.0**	**0.0**	**30.0**	**10.0**	**59.3**	**547.5**	**0.0**	**0.0**	**80.6**	**0.0**	**727.3**
DARPA	FY2017 Actual	30.8	0.0	289.4	0.0	5.1	0.0	0.0	100.8	23.7	0.0	449.8
	FY2018 Estimate	*62.0*	*0.0*	*301.9*	*0.0*	*5.1*	*0.0*	*0.0*	*104.1*	*22.6*	*0.0*	*495.8*
	FY2019 Request	**69.4**	**0.0**	**275.6**	**0.0**	**5.1**	**0.0**	**0.0**	**76.6**	**49.5**	**0.0**	**476.1**
NASA	FY2017 Actual	5.5	6.1	0.5	0.0	15.5	59.7	208.0	2.7	37.2	12.4	347.4
	FY2018 Estimate	*3.1*	*1.5*	*0.0*	*0.0*	*16.6*	*54.3*	*114.1*	*2.4*	*52.7*	*9.6*	*254.3*
	FY2019 Request	**0.4**	**0.2**	**0.0**	**0.0**	**18.8**	**59.0**	**129.8**	**2.1**	**51.7**	**5.0**	**267.1**
NIST	FY2017 Actual	7.3	12.6	70.3	4.1	5.3	9.4	7.2	13.9	10.4	2.4	142.8
	FY2018 Estimate	*7.3*	*13.0*	*70.3*	*4.1*	*5.3*	*9.4*	*7.2*	*13.9*	*10.4*	*2.4*	*143.3*
	FY2019	**6.9**	**10.5**	**68.4**	**4.1**	**3.8**	**8.9**	**7.3**	**12.6**	**6.6**	**2.4**	**131.6**
NOAA	FY2017 Actual	0.2	0.0	0.0	0.0	0.0	49.8	0.0	0.0	3.3	3.7	57.0
	FY2018 Estimate	*0.2*	*0.0*	*0.0*	*0.0*	*0.0*	*49.5*	*0.0*	*0.0*	*3.3*	*3.7*	*56.7*
	FY2019 Request	**0.2**	**0.0**	**0.0**	**0.0**	**0.0**	**35.4**	**0.0**	**0.0**	**3.3**	**3.7**	**42.6**
DHS	FY2017 Actual	0.0	0.0	52.0	0.0	0.0	0.0	0.0	3.5	0.0	0.0	55.5
	FY2018 Estimate	*4.2*	*0.0*	*43.9*	*0.0*	*0.0*	*0.0*	*0.0*	*4.0*	*0.0*	*0.0*	*52.1*
	FY2019 Request	**0.0**	**0.0**	**41.4**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**41.4**
NIJ	FY2017 Actual	0.2	0.0	0.5	0.0	0.2	0.0	0.0	1.3	0.0	2.0	4.2
	FY2018 Estimate	*0.0*	*0.0*	*0.0*	*0.0*	*0.3*	*0.0*	*0.0*	*2.0*	*0.0*	*2.3*	*4.6*
	FY2019 Request	**0.0**	**0.0**	**0.0**	**0.0**	**0.3**	**0.0**	**0.0**	**2.0**	**0.0**	**2.3**	**4.6**
DOT	FY2017 Actual	0.0	0.6	0.0	0.0	0.0	0.0	0.0	0.0	0.8	0.0	1.4
	FY2018 Estimate	*0.0*	*1.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*1.7*	*0.0*	*2.7*
	FY2019 Request	**0.0**	**1.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**1.7**	**0.0**	**2.7**
NARA	FY2017 Actual	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2	0.0	0.0	0.2
	FY2018 Estimate	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.2*	*0.0*	*0.0*	*0.2*
	FY2019 Request	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.2**	**0.0**	**0.0**	**0.2**
AHRQ	FY2017 Actual	16.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.5
	FY2018 Estimate	*16.4*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*16.4*
	FY2019 Request	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
EPA	FY2017 Actual	0.0	0.0	0.0	0.0	3.5	3.0	0.0	0.0	0.0	0.0	6.5
	FY2018 Estimate	*0.0*	*0.0*	*0.0*	*0.0*	*3.5*	*3.0*	*0.0*	*0.0*	*0.0*	*0.0*	*6.5*
	FY2019 Request	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
DOE/NNSA	FY2017 Actual	0.0	0.0	0.0	3.5	30.0	0.0	0.0	0.0	0.0	0.0	33.5
	FY2018 Estimate	*0.0*	*0.0*	*0.0*	*3.5*	*40.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*43.5*
	FY2019 Request	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
Total[b]	FY2017 Actuals	731.2	138.0	744.6	168.0	323.5	1,225.4	387.7	683.2	434.1	290.5	5,126.4
Total[b]	*FY2018 Estimate[a]*	*754.2*	*138.8*	*783.2*	*160.9*	*327.0*	*1,195.2*	*301.2*	*705.9*	*489.6*	*295.5*	*5,151.5*
Total[b]	**FY2019 Request[e]**	**744.0**	**139.1**	**739.7**	**156.6**	**284.9**	**1,353.3**	**342.6**	**710.6**	**522.8**	**283.9**	**5,277.6**

BUDGET TABLE NOTES (see Table 1 on previous page)

a. Figures in the table's 2018 rows reflect the annualized levels under the FY2018 Continuing Resolution.

b. Totals might not sum exactly due to rounding.

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

d. The DOE budget includes funding from DOE's Office of Science (DOE/SC) and Office of Cybersecurity, Energy Security, and Emergency Response (DOE/CESER, formerly part of the Office of Electricity Delivery and Energy Reliability). The DOE/National Nuclear Security Administration (NNSA) budget is listed separately.

e. FY2019 numbers contain updates from the Addendum to the FY2019 Budget (https://www.whitehouse.gov/wp-content/uploads/2018/02/Addendum-to-the-FY-2019-Budget.pdf) for agencies whose NITRD budgets were affected.

Budget Analysis by Agency

The following budget analysis notes changes of investment greater than $10 million, by agency, between the FY2018 Estimate and the FY2019 Presidential Budget Request. Because no final appropriations were enacted at the time of NITRD budget data collection, the FY2018 estimates reflect annualized amounts provided in the Continuing Appropriations Act, 2018, and therefore are not final.

AHRQ: The decrease of $16.4 million is due to no funds being requested for CHuman.

DARPA: The decrease of $19.7 million is due to decreases of $26.3 million in CSP due to the completion of the Edge-Directed Cyber Technologies for Reliable Mission Communication, Plan X, and Supply Chain Hardware Integrity for Electronics Defense programs in 2018; and of $27.5 million in LSDMA due to the completion of the Mining and Understanding Software Enclaves, Big Mechanism, and Deep Extraction from Text programs in 2018, partially offset by an increase of $26.9 million in LSN for scale-up of the Secure Handhelds on Assured Resilient Networks at the Tactical Edge and Network Universal Persistence programs, with smaller increases in other PCAs.

DHS: The $10.7 million decrease is due to smaller requests in CHuman, CSP, and LSDMA.

DoD: The increase of $104.9 million is primarily due to increases of $39.3 million in LSDMA, $32.2 million in IRAS, and $10 million in CHuman, with smaller increases and decreases in other PCAs.

DOE: The increase of $165.0 million is due to increases in funding in HCIA for upgrades at the Leadership Computing Facilities and in EHCS for quantum information science and quantum networking research, with smaller increases and decreases in other PCAs.

DOE/NNSA: The decrease of $43.5 million is due to a decrease of $40.0 million in EHCS of the DOE Exascale Computing Project (ECP) PathForward program, with smaller decreases in other PCAs.

NASA: The increase of $12.8 million is due to an increase of $15.7 million in IRAS, which is primarily related to investments in In-space Robotic Manufacturing and Assembly, with smaller increases and decreases in other PCAs.

NIST: The decrease of $11.7 million is due to smaller requests in CHuman, CNPS, CSP, HCIA, LSDMA, and LSN.

NOAA: A decrease of $14.1 million for HCIA activities is due to two decreases in NOAA's original FY2018 Budget Request published in October 2017 rather than to a decrease in the FY2019 Budget Request: (1) elimination of $10 million in funding in FY2018 (received but not requested in FY2017) for a high-performance computing partnership with Mississippi State University's Northern Gulf Institute, and (2) a $4 million reduction in the original FY2018 funding requested by the National Weather Service.

NSF: NSF investment in NITRD is reduced slightly (-2.6%) across all the PCAs, with slight increases and decreases within the PCAs reflecting evolving priorities.

3. Program Component Areas

Section 3 contains one subsection for each PCA, including the official PCA definition and planned FY2019 Federal R&D activities—Strategic Priorities, Key Programs, and Key (interagency) Coordination Activities—coordinated by each NITRD IWG reporting under that PCA. Names of programs use title case, whereas descriptions of types of programs use sentence case. Agencies are listed in alphabetical order, not in order of leadership, level of effort, or funding.

Computing-Enabled Human Interaction, Communication, and Augmentation (CHuman) PCA

CHuman involves R&D of information technologies that enhance human ability to interact with IT systems, others, and the physical world, including R&D in social computing, human-human and human-machine interaction and collaboration, rational decision-making, command and control, and human and social impacts of IT.

The Social Computing IWG reports its activities under the CHuman PCA.

Social Computing (SC) IWG

***Participating Agencies*: Air Force, Army, DARPA, DOE/EM, Navy, NIH, NIST, NRC, NSF**

The SC IWG coordinates Federal R&D in information technologies focused on how people interact with and through IT in applications that include military action, disaster response, healthcare, innovation, and commerce. SC also considers the impacts of IT on society broadly, in terms of identifying and mitigating the potential harm and maximizing the benefit of socially interactive IT applications ranging from artificial intelligence (AI) and automation, to information-sharing and social networks.

Strategic Priorities

- **Collaborative support:** Develop responsive and smart social environments at scales from teams to communities that integrate ubiquitous computing, networking technologies, data analytics, knowledge representation, and understanding of human behavior to accelerate innovation in disperse teams.
- **Human-automation interaction:** Facilitate interaction between humans and intelligent systems (e.g., robots, intelligent agents, autonomous vehicles, and systems using machine learning), working toward common goals.
- **Social innovation:** Support collective innovation and creativity, both in material products (e.g., digital fabrication, and crowdsourcing of design challenges) and intellectual products (e.g., open source software and citizen science).
- **Social informatics:** Advance models, systems, and interfaces that manage information, veracity, and dissemination online in disasters; in addition, develop models, systems, and interfaces capable of detecting adversaries' malicious attempts to disseminate misinformation.

Key Programs

- **Sensing and modeling social dynamics:** Advance the measurement of emerging social processes and interdependencies among social, natural, and physical systems through three Multidisciplinary University Research Initiative projects: Social Media Analytics, Cybersecurity, and Interdependencies among Social and Natural Systems. *ARO*
- **Social computing:** Improve situational awareness (including social media and network analytics) and develop tools to rapidly assess situations. *ARO, DARPA*

- **Human-agent teaming:** Increase the effectiveness of interactions between human and nonhuman systems. *ARL, ARO*
- **Human variability:** Understand the impact that differences among humans have on interaction and performance within and between groups. *ARO*
- **Complexity modeling:** Capture the interdependencies across different systems that lead to unexpected risks and failures, including complex, human-in-the-loop systems. *ARO*
- **Historically Black Colleges and Universities and Minority-Serving Institutions (HBCU/MSI) STEM programming:** Support the Undergraduate Research Apprenticeship and HBCU/MSI Supplement for Basic Research programs. *ARO*
- **Cyber-human systems**: Improve the fundamental understanding of how, and the processes by which, interactive systems should be designed to achieve human-computer symbiosis and computer-mediated human communication, collaboration, and competition. *ARO, DARPA, NSF*
- **Cyberlearning for Work at the Human-Technology Frontier:** Educate learners of all ages in STEM so that they are equipped with the IT skills required for future jobs, including functioning in highly technological environments and in collaboration with emerging intelligent systems. *NSF*
- **National Robotics Initiative 2.0:** Integrate ubiquitous and collaborative robots that work seamlessly beside or cooperatively with people to assist humans in every aspect of life. *DoD, DOE/EM, NASA, NSF, USDA*
- **Robust Intelligence:** Support and advance intelligent systems that operate in complex, realistic contexts. *DARPA, NSF*
- **Smart and Autonomous Systems:** Develop intelligent physical systems that robustly think, act, learn, and behave ethically. *NSF, industry partners*
- **Smart and Connected Communities:** Address the technological and social dimensions, and their interactions, in smart community environments. *NSF*
- **Information Integration and Informatics:** Realize the transformative potential of data, information, and knowledge in this digital and interconnected world. *ARO, NSF*
- **Algorithmic Foundations:** Focus on information transmission and trustworthiness. *NSF*

Key Coordination Activities

- **Social complexity and social dimensions of cybersecurity:** Program/project review and co-management via co-sponsored workshops, project and program review panels comprising multiagency representatives, co-authorship of multiagency extramural research opportunities, such as the Multidisciplinary University Research Initiative Program administered by the Office of the Under Secretary of Defense, Research & Engineering. *ARO, DARPA, DTRA, OUSD(R&E)*
- **Social computing and network analytics:** Joint program/project review and planning to avoid program duplication in support of extramural basic research that models human interaction through social networks (e.g., social media, face-to-face interaction), the effect of social networks on individual and group behaviors, and the consequences of those behaviors; efforts include co-reviewing research proposals, collaboratively funding innovative, high-impact extramural research, and co-managing research programs across agencies. *ARO, DTRA, DARPA*
- **Minerva Research Initiative:** Social science research, including on cyber, social media, and autonomous systems. *AFOSR, ARO, ONR, OUSD(R&E)*
- **Public Participation in Scientific Research:** Public participation in scientific research that increases public science literacy through informal science education, for example, efforts to increase participation of underserved minority groups in STEM education and research, and development of the program for Science and Technology Information Exchange to communicate research findings to the public. *AFOSR, ARO, DOE/EM, NIH, NSF, ONR, OUSD(R&E)*

Computing-Enabled Networked Physical Systems (CNPS) PCA

CNPS involves R&D for information technology-enabled systems that integrate the cyber/information, physical, and human worlds, including R&D of cyber-physical systems (CPS), Internet of Things (IoT), and related complex, high-confidence, networked, distributed computing systems.

The following groups report their activities under the CNPS PCA:

- Cyber-Physical Systems IWG, including the Smart Cities and Communities Task Force
- High Confidence Software and Systems IWG

Cyber-Physical Systems (CPS) IWG

***Participating Agencies*: Air Force, DHS, DOE/EERE, DOE/OE, DOS, EPA, FAA, FDA, FHWA, HUD, ITA, NASA, NIFA, NIH, NIST, NRC, NSA, NSF, NTIA, OSD, USPS**

The CPS IWG coordinates Federal R&D in cyber-physical systems and related areas, including Smart Cities and Communities and the Internet of Things, that fall under the broader umbrella of smart, networked sociotechnical systems. The Smart Cities and Communities (SCC) Task Force is a body under the CPS IWG that coordinates Federal action and facilitates partnerships among industry, academia, government, and communities to ensure that communities in all settings and at all scales have access to CPS and IoT technologies and services. The R&D coordination enabled by the CPS IWG and SCC Task Force promotes U.S. technological leadership and global competitiveness in sectors that include security, energy, transportation, manufacturing, and health.

Strategic Priorities

- **Science and technology for building cyber-physical systems:** Develop the core science and engineering of complex CPS technologies by providing the unified foundations, models and analysis tools, system capabilities, standards for interoperability, and architectures that enable innovation in highly dependable, cyber-enabled engineered and natural systems. Create measurement solutions, reliable testing and certification methods, and robust implementation practices for scalable, interoperable, safe, secure, and resilient CPS technologies.
- **Smart Cities and Communities:** Convene stakeholders to identify challenges, enable solutions, determine best practices, and support growth of the SCC R&D community.
- **Manufacturing systems:** Coordinate public and private stakeholders to effectively leverage advanced IT methods to improve the productivity and capabilities of U.S. industry.
- **Cybersecurity and privacy:** Minimize vulnerabilities and protect privacy in CPS and IoT technologies, focusing on built-in data security, controlled sharing, and trustworthiness.
- **Autonomous mobility systems:** Support R&D of hardware, software, algorithms, and models to enable verifiable autonomous mobility systems across multiple modes that are safe and reliable.
- **Human health, wellbeing, and safety:** Create tools and devices to measure and understand the brain, leverage smart technologies for health assessment and assistance, develop and deploy technologies for mobility-impaired persons, and study human-CPS technology integration.
- **Education and workforce development and impact:** Create new curricula that integrate CPS theory and methodology across both the physical and cyber disciplines, support authentic CPS research experiences, integrate community partners into award programs to support CPS workforce development, and study the impact of CPS technology on existing workforce sectors.

Key Programs

- **Cyber-Physical Systems:** Explore the fundamental scientific, engineering, and technological principles that underpin the integration of cyber and physical elements; develop safety models and designs for cyber-physical systems; and develop open CPS testbed platforms. This includes joint R&D proposal evaluation. *FDA, FHWA, ITS JPO, NASA, NIFA, NIH, NSF*
- **Smart and Connected Communities:** Support development and integration of smart and connected communities and their underlying technologies (e.g., sensor networks, data analytics, and control and automation). *FDA, NASA, NIFA, NIH, NIST, NSF, NTIA, OSD*
- **Platforms for Advanced Wireless Research:** Enable experimentation of robust new wireless devices, communications techniques, networks, systems, and services, in support of future smart and connected communities. *NSF*
- **Global City Teams Challenge (GCTC):** Facilitate collaboration among stakeholders to promote replicable, scalable, and sustainable models for incubation and deployment of interoperable, standards-based IoT solutions, and demonstrate their measurable benefits in smart cities and communities. *DOS, DOT, ITA, NIST, NSF, NTIA*
- **Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative:** Support research and training to develop and test new tools and devices to understand neurocircuitry. *DOD, FDA, IARPA, NIH, NSF*
- **Smart City Challenge:** Support fundamental R&D to address mobility challenges faced by cities and communities and demonstrate how advanced data and intelligent transportation systems technologies can address challenges in safety, mobility, sustainability, prosperity, and the environment. *DOE, ITS JPO, NSF, other CPS IWG agencies*
- **Advanced Transportation and Congestion Management Technologies Deployment Program:** Promote transition to practice of CPS technologies for vehicle automation and infrastructure, data collection and management, and smart cities. *FHWA*
- **Cyber-Physical Systems Security:** Support R&D with a focus on transition to practice to promote best practices and develop new tools and techniques in CPS security. *FDA, NSF*
- **Air traffic management and operations:** Develop a services-based architecture for unmanned aerial vehicle traffic management and operations through R&D in communications, cybersecurity, and development of prototypes and testbeds. *FAA, NASA, other CPS IWG agencies*
- **IoT Cybersecurity:** Support development and application of standards, guidelines, and tools to improve the cybersecurity of connected devices and their deployed environments. *DoD, NIST*
- **Transactive Energy Modeling and Simulation Challenge for the Smart Grid:** Develop simulation-platform-agnostic and interoperable modeling approaches to study distribution grid management in emerging, market-enabling grid architectures. *NIST*

Key Coordination Activities

- **Principal Investigator (PI) meetings:** Annual forums for all stakeholders to review research developments, identify new and emerging applications, and discuss science and technology gaps and barriers. *AFRL, FDA, FHWA, NASA, NIFA, NIH, NIST, NSF, NTIA, OSD*
- **GCTC Expo:** Annual event to highlight public-private partnerships for replicable and trustworthy smart city and community applications. *DOS, DOT, ITA, NIST, NSF, NTIA*
- **US Ignite Application Summit:** Annual public forum for demonstration of advanced applications that take advantage of next-generation networking technology and support future smart and connected communities; the Summit bridges academic research and community stakeholders for increased impact. *NSF*

High Confidence Software and Systems (HCSS) IWG

***Participating Agencies*: Air Force, Army, EPA, FAA, FDA, FHWA, ITS JPO, NASA, Navy, NIFA, NIH, NIST, NOAA, NRC, NSA, NSF, OSD**

The HCSS IWG coordinates Federal R&D on next-generation engineered systems that depend on cyber control and require very high levels of system assurance, including military and commercial aircraft and vehicles, critical infrastructure, and other safety-critical systems, both human-guided and autonomous.

Strategic Priorities

- **System assurance:** Pursue foundational and applied research and standards to mature the scientific basis for designing, building, securing, and verifying complex CPS and IoT technologies; develop and promote use of formal methods in diverse applications; secure national assets by providing means to minimize exploitable vulnerabilities in cyber-enabled systems; and enable scaling, interoperability, calibration, and validation of mission-related systems.
- **Assured autonomous and artificial intelligence technologies:** Support the application of autonomous and AI technologies, especially in safety-critical and high-dependability applications, by enabling cyber-enabled physical systems to self-protect at machine speed and scale; automate vulnerability discovery and patching; and assure autonomous mobility systems.
- **Transition to practice:** Facilitate the transition of new HCSS tools and technologies from laboratories to the private sector to reduce the time to design, build, and verify complex systems; and promote the development and public use of testbeds for HCSS R&D.
- **Education and workforce development:** Develop new curricula that integrate HCSS theory and methodology, promote authentic research experiences for students, and increase the application of formal methods in software engineering through education and tool development.

Key Programs

- **Cyber-Physical Systems:** Explore the fundamental scientific, engineering, and technological principles that underpin the integration of cyber and physical elements, particularly how to design CPS to be safe, secure, and resilient in unanticipated and rapidly evolving environments, and how to reduce the time to verify and certify large, complex CPS. *AFRL, DOT, FDA, NASA, NIFA, NIH, NSF*
- **Software Assurance Metrics and Tool Evaluation:** Develop software assurance reference datasets that enable developers to reduce vulnerabilities in tools, including the Software Assurance Reference Data Set, automated combinatorial testing tools, the National Vulnerability Database, and the Bugs Framework. *FDA, NIST, NSA, NSF*
- **CPS for manufacturing:** Improve system reliability and production quality, and reduce cost; develop new methods for detecting malicious interference in cutting-edge manufacturing processes, including additive manufacturing; and promote designed-in security of critical manufacturing processes and infrastructure. *NSF*
- **Cybersecurity for smart manufacturing systems:** Quantify the impact of cybersecurity technologies on performance, including of industrial control systems, and develop implementation guidelines for the NIST Cybersecurity Framework Manufacturing Profile. *NIST*
- **Artificial intelligence and machine learning (AI/ML) for safety- and mission-critical applications:** Explore new techniques for assuring and engineering trusted AI-based systems, including development of shared public datasets and environments for AI/ML training and testing, and development of standards and benchmarks for assessing AI technology performance. *NIST, NSA, NSF*

- **Foundational autonomy for manned/unmanned systems:** Enable increasingly autonomous manned-unmanned teams performing highly agile missions utilizing heterogeneous platforms by developing foundational autonomy in an open, flexible, and assured framework. *AFRL, NASA*
- **Boutique analysis:** Improve the assurance of security-critical algorithms, protocols, software, and hardware relevant to national security systems through research to develop foundational technology and techniques to apply that technology to specific niche problem areas. *NSA*
- **Centaur-styled analysis:** Develop analysis technologies that leverage the best of both human and machine capabilities, automating previously difficult and time-consuming tasks, and enabling human analysts to conduct sophisticated operations in real time. Research focuses on realizing automation within vulnerability discovery and mitigation during the careful and incremental transition to assured autonomy across vulnerability processes. *NSA*
- **Assumption-driven design:** Overcome obstacles to the effective use and scaling of techniques for trustworthy system design and refinement that systematically identify, track, and validate security-relevant assumptions. *NSA*
- **Exploratory Advanced Research Program:** Support long-term, high-risk research in connected highway and vehicle system concepts with the potential to transform transportation systems. *FHWA*
- **Advanced Transportation and Congestion Management Technologies Deployment Program:** Develop model deployment sites for large-scale installation and operation of advanced transportation technologies, which may include complex software systems, to improve safety, efficiency, performance, interoperability, and infrastructure return on investment. *FHWA, ITS JPO*
- **Connected vehicle (CV) pilots and demonstrations:** Demonstrate CV and smart infrastructure technology and applications under real-world scenarios. *ITS JPO*
- **Urban Air Mobility Challenge:** Realize personal and autonomous air vehicles through R&D on assurance for both current-generation and emerging capabilities, certification challenges, and assured detect-and-avoid algorithms for unmanned aerial systems; and R&D for autonomous systems. *FAA, NASA*
- **Scholar-in-Residence:** Investigate the scientific and engineering issues in emerging trends in medical device technology. *FDA, NSF*

Key Coordination Activities

- **PI meetings:** Forums for all stakeholders to review research developments, identify new applications, and discuss science and technology gaps and barriers. *AFRL, FDA, FHWA, NASA, NIFA, NIH, NIST, NSF, NTIA, OSD*
- **HCSS conferences:** Support for collaboration with the annual HCSS Conference, Verification and Validation Summit, NASA Formal Methods Symposium, and Safe and Secure Software and Systems Symposium. *AFRL, FAA, NASA, NSA, NSF*
- **Joint R&D proposal evaluations:** Promotion of portfolio synergies. *AFRL, NASA, NSA, NSF*

Cyber Security and Privacy (CSP) PCA

CSP involves R&D to protect information and information systems from cyber threats and to prevent adverse privacy effects arising from information processing, including R&D to deter, detect, prevent, resist, respond to, recover from, and adapt to threats to the availability, integrity, and confidentiality of information and information systems, as well as R&D of privacy-protecting information systems and standards.

The following groups report their activities under the CSP PCA:

- Cyber Security and Information Assurance IWG
- Privacy Research and Development IWG

Cyber Security and Information Assurance (CSIA) IWG

***Participating Agencies*: Air Force, Army, DARPA, DHS, DOE/CESER, DOT, IARPA, Navy, NIH, NIJ, NIST, NRC, NSA, NSF, OSD, Treasury**

The CSIA IWG coordinates Federal R&D to protect information and information systems from cyber threats. This R&D supports the security and safety of U.S. information systems that underpin a vast array of capabilities and technologies in many sectors, from power generation, transportation, finance, healthcare, and manufacturing, to national security.

Strategic Priorities

Federal strategic priorities for cybersecurity research are outlined in the 2016 *Federal Cybersecurity Research and Development Strategic Plan*.[5] The strategic plan provides priorities for cybersecurity R&D in alignment with the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[6] which provides guidance on managing and reducing cybersecurity risk confronted by businesses and organizations. Guided by the strategic plan, CSIA agency investments for FY2019 will focus on key research in the following priority areas:

- **Deter:** The ability to efficiently discourage malicious cyber activities by increasing the costs, risks, and uncertainty to adversaries and diminishing their spoils.
- **Protect:** The ability of components, systems, users, and critical infrastructure to efficiently resist malicious cyber activities and to ensure confidentiality, integrity, availability, and accountability.
- **Detect:** The ability to efficiently detect, and even anticipate, adversary decisions and activities, given that systems should be assumed to be vulnerable to malicious cyber activities.
- **Adapt:** The ability to dynamically adapt to malicious cyber activities by reacting to disruption, recovering from damage, and adjusting to be able to thwart similar future activity.

Key Programs

- **Deter**: Develop methods to assess adversary levels of effort, results, and risks; provide for effective and timely attribution of malicious cyber activities to their sources; design robust investigative tools; and support information sharing for attribution. Key activities include:
  - Cyber deception. *ARL, CERDEC, ONR*
  - Cyber attribution. *DARPA*
  - Malware analysis at scale. *DHS*
  - Proactive cyber defense. *AFRL, ARL, CERDEC*

[5] https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf
[6] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

  - Situational awareness and incident response in cloud environments. *DHS*
- **Protect:** Develop technologies that limit software and system vulnerabilities through design, construction, and verification, and that enforce security though authentication, access control, and cryptography. Key activities include:
  - Automated and autonomous cyber defense and operations. *AFRL, DARPA, ONR*
  - Assured systems engineering. *AFRL, DARPA*
  - Resilient cyber and cyber-physical systems. *ARL, CERDEC, DARPA, DOE/CESER, NIST, NSA, NSF, ONR*
  - Application, network, mobile, and hardware security. *AFRL, ARL, CERDEC, DARPA, DHS, DOE/CESER, NIST*, *NSA, NSF, ONR, OSD*
  - Configuration and vulnerability management. *NIST*
  - Deployable collaboration environment. *DHS*
- **Detect:** Develop technologies to ensure that system and network owners and users have situational awareness and understanding of ongoing (authorized and unauthorized) activities and can reliably detect malicious cyber activities. Key activities are:
  - Cyber situational awareness. *AFRL, ARL, CERDEC, DARPA, DHS, DOE/CESER, HPCMP*
  - Botnet and malware detection and mitigation. *DHS, NIST*
- **Adapt:** Develop technologies to provide real-time assessment of system changes and anomalies, provide adaptive response to actual and emerging disruptions, and enable automated recovery. Key activities include autonomous, agile, and biologically resilient cyber technologies. *AFRL, CERDEC, DARPA, DHS, DOE/CESER, NIST, ONR, OSD*
- **Scientific foundations:** Establish the theoretical, computational, and data mining foundations needed to address future threats. Key activities include:
  - Quantum-based security. *AFOSR, DOE/CESER, NIST*
  - Cryptography. *NIST, NSA, NSF, ONR*
  - Formal methods. *AFRL, DARPA, NSA, NSF, OSD*
- **Risk management:** Develop techniques for assessment of an organization's assets, vulnerabilities, and potential threats so that security investments can be risk-informed. Key activities include cyber risk analysis. *ARL, DHS, DOE/CESER, NIST*
- **Human aspects:** Improve understanding of how users, defenders, and adversaries interact with information technologies, and of the social, behavioral, and economic aspects of cybersecurity. Key activities include:
  - Sociotechnical dimensions. *ARL, DARPA, NSF, OSD*
  - Usability of security. *NIST*
- **Workforce development:** Foster programs in cybersecurity education, training, and professional development to sustain cybersecurity innovations by the national workforce. Key activities include:
  - Cyber competitions. *NIST*
  - Cybersecurity education. *AFRL, NIST, NSA, NSF*
- **Transition to practice**: Support testing, evaluation, and commercialization activities that engage the private sector; and streamline and accelerate the acquisition process. Key activities include:
  - Transition-to-practice programs. *DOE/CESER, NIST, NSF, OSD*
  - Silicon Valley Innovation Program. *DHS*
- **Research infrastructure:** Maintain and develop tools, test environments, and datasets at the right scale and fidelity to support a broad range of experimentation and analysis across the full range of cybersecurity challenges. Key activities include:

- Testbeds. *AFRL, ARL, DOE/CESER, NIST, NSF, ONR*
- Data repositories. *NSF*

Key Coordination Activities

- **Federal Cybersecurity R&D Strategic Plan Implementation Roadmap:** As directed by the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), the *Implementation Roadmap for the Federal Cybersecurity R&D Strategic Plan* is updated annually by the CSIA IWG. The FY2019 Implementation Roadmap is provided on the NITRD website.[7] *All CSIA IWG Agencies*
- **Collaborative research:**
  - Cyber-Security Collaborative Research Alliance. *ARL, CERDEC*
  - Cyber Resilient Energy Delivery Consortium. *DOE/CESER*
  - Cyber-physical systems security.*DOT, NIST, NSF*
  - National Cybersecurity Center of Excellence. *NIST*
- **Agency-sponsored conferences and workshops:**
  - Annual cyber technology demonstrations. *DARPA, NIST, NSA, OSD*
  - Cyber and cyber-physical security public working groups. *NIST*
  - National Initiative for Cybersecurity Education Conference and Expo. *DHS, NIST, NSA, NSF*
  - Cybersecurity research workshops. *NSF*
- **Technical standards:**
  - Cryptographic standards. *NIST, NSA*
  - Internet Engineering Task Force public working groups. *DHS, NIST, NSA, OSD*
- **DoD Cyber community of interest:** Oversight and coordination among DoD cyber science and technology programs. *AFRL, ARL, CERDEC, DARPA, NSA, ONR, OSD*
- **Cyber education:**
  - Centers of Academic Excellence. *NSA*
  - CyberCorps: Scholarship for Service, Advanced Technological Education. *NSF*
  - National Initiative for Cybersecurity Education. *DHS, NIST, NSA, NSF, OSD*
- **International collaborations:**
  - Science programs with Israel, Netherlands, and Brazil. *NSF*
  - Joint cybersecurity R&D programs with Australia, Canada, Israel, Japan, Netherlands, New Zealand, Singapore, Sweden, and the United Kingdom. *DHS*
  - Cryptographic algorithm validation with Canada. *NIST*
  - The Technical Cooperation Program—Command, Control, Communications, and Information Systems Group of Australia, Canada, New Zealand, the United Kingdom, and the United States. *AFRL, ARL, CERDEC, NSA, ONR, OSD*
  - Joint funding with South Korea's Ministry of Science. *AFRL*

Privacy Research and Development IWG

***Participating Agencies*: Air Force, Army, Census, DARPA, DHS, FCC, FTC, NARA, Navy, NIH, NIST, NSA, NSF, NTIA, OSD**

The Privacy IWG coordinates Federal R&D aimed at preventing adverse privacy effects arising from information processing, including R&D of privacy-protecting information systems and standards. This R&D supports advances in large-scale data analytics that, for example, can improve healthcare, eliminate barriers to education and employment, and increase efficiencies in the transportation and

[7] https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf

financial sectors, while minimizing risks to individual privacy and possible harms such as discrimination, loss of autonomy, and economic losses. The following summarizes Privacy activities, as outlined in the 2016 *National Privacy Research Strategy*.[8]

Strategic Priorities

- Foster a multidisciplinary approach to privacy research and solutions.
- Understand and measure privacy desires and impacts.
- Develop system design methods that incorporate privacy desires, requirements, and controls.
- Increase transparency of data collection, sharing, use, and retention.
- Assure that information flows and uses are consistent with privacy rules.
- Develop approaches for remediation and recovery.
- Reduce privacy risks of analytical algorithms.

Key Programs

- **Privacy and data analytics:**
  - Develop practical approaches to implementing privacy protections in data analytics systems, in statistical data provided by the Federal Government, and in multiparty computation. *Census, DARPA, DHS, NSA, NSF*
  - Formal Privacy for the 2020 Census and Formal Privacy for the American Community Survey. *Census*
  - Improve privacy of biomedical data. *NIH*
- **Privacy engineering:** Develop standards-based tools and practices to understand and mitigate privacy risks and integrate privacy controls into information systems. *NIST*
- **Privacy in medicine:** Protect genetic privacy, identity, and privacy of electronic health records; and improve privacy-preserving technologies for medical research. *NIH, NIST, NSF*
- **Privacy for mobile and IoT:** Address privacy concerns with networking, mobile computing, sensor platforms, unmanned aircraft systems, and cyber-physical systems. *DHS, NIST, NSF*
- **Explorations in privacy:** Conduct research to advance the technical, social, behavioral, economic, and mathematical understanding of privacy. *NSF*
- **Transition to practice:** Transition privacy solutions to the marketplace. *DHS, NIST*

Key Coordination Activities

- **Workshops:** Annual workshops on privacy research topics; e.g., past workshops have examined such topics as privacy controls, algorithmic transparency, and consumer privacy protections. *FTC, NIST, NSF*
- **Technical privacy guidelines:** Development and coordination of recommendations, guidelines, and standards for privacy-preserving technologies and privacy risk assessment methodologies (e.g., NIST SP 800-53, NIST SP 800-122, and NIST IR 8053). *DHS, DoD, NIST, ODNI*
- **Privacy risk assessments:** Implementation of privacy risk assessment of Federal agencies' systems. *NIST, NITRD Agencies*
- **International collaborations:** International engagements and co-funding activities in security and privacy with Australia, Brazil, Canada, Israel, Japan, Netherlands, New Zealand, Singapore, Sweden, and the United Kingdom. *DHS, NSF*

[8] https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf

Education and Workforce (EdW) PCA

EdW involves R&D using information technology to improve education and training, including IT to enhance learning, teaching, assessment, and standards, as well as preparation of next-generation cyber-capable citizens and professionals.

EdW activities are coordinated directly through the NITRD subcommittee and through other IWGs as appropriate. Agencies also coordinate related activities more broadly through the NSTC Committee on Science, Technology, Engineering, and Math Education.

The agencies that report budgets for this PCA are as follows:

***Participating Agencies*: DHS, DOC, DOE/SC, DOL, ED, FCC, NASA, Navy, NIH, NIST, NSA, NSC, NSF, ODNI, OPM**

Agency and interagency activities reported under the EdW PCA leverage IT to improve the learning and teaching of America's technically skilled workforce, and to prepare all Americans—from urban to rural, with a special emphasis on women and other underrepresented groups—for an increasingly digital-reliant society.

Strategic Priorities

- **Access to advanced technical education:** Create new educational opportunities in IT at all levels from kindergarten on up to ensure the flow of technically skilled American teachers and workers, advance the skillsets of the current workforce to fill near-term shortages of needed researchers and practitioners, and improve the breadth and depth of capabilities in users of IT tools and methods.
- **Lifelong learning:** Design effective lifelong learning programs to help Americans keep up with technological and societal changes, to ensure that the domestic workforce is available and qualified for the jobs of the future.
- **Interagency and multisector coordination:** Coordinate and collaborate among Federal agencies and the business and educational communities, including nonprofits, in developing educational programs, tools, and technologies that enable, sustain, and support a persistent and robust education ecosystem for all Americans.
- **Assessment:** Develop quantitative and complementary qualitative methods for data collection and holistic analysis to evaluate the effectiveness of key programs supporting this request relative to defined metrics.

Key Programs

- **K–12 computer science (CS) education:** Continue efforts to build on the K–12 CS education knowledge base through support for researcher-practitioner partnerships that expand CS education to all American classrooms. *NSF*
- **CS undergraduate education:** Work with colleges and universities to explore novel approaches for CS undergraduate education programs that are responsive to both the large influx of American students and the increased multidisciplinary interests of many of those students. *NSF*
- **Cyberlearning for Work at the Human-Technology Frontier:** Educate learners of all ages in STEM so that they are equipped with the IT skills required for future jobs, including functioning in highly technological environments and in collaboration with emerging intelligent systems. *NSF*
- **National Initiative for Cybersecurity Education (NICE):** Promote and energize a robust network and an ecosystem of cybersecurity education, training, and workforce development. Led by NIST, the NICE partnership between government, academia, and the private sector

(including industry partners) builds on existing successful programs, facilitates change and innovation, and brings leadership and vision to increase the number of skilled cybersecurity professionals helping to keep the Nation secure. *DHS, DOC, DoD, DOE/SC, DOL, ED, FCC, NIST, NSA, NSC, NSF, ODNI, OPM*

- **Increasing the rigor and reproducibility of NIH research:** NIH is creating training materials on scientific rigor for graduate students and fellows and working to improve data sharing and accessibility to improve reproducibility in publications. *NIH*
- **Supporting new NIH investigators:** Through the Next Generation Researchers Initiative, established by the 21st Century Cures Act, NIH is supporting new investigators, aiming for earlier research independence in the biomedical workforce. *NIH*

Key Coordination Activities

- **NSTC Federal Coordination in STEM Education IWG on K–12 CS Education (co-chaired by NSF and ED):** Enable coordination across all IWG member agencies, including NITRD agencies, and the private sector in support of growing the K–12 CS education knowledge base and expanding access to K–12 CS education at all American schools. *ED, NSF, others*
- **DoD STEM strategy:** Focus on developing and retaining a diverse STEM-proficient workforce and network to drive science and technology innovation, including driving the highest standards of scientific discovery. *DoD, ONR*
- **NICE Strategic Plan:** Continue implementation of the strategy required by the Cybersecurity Enhancement Act of 2015. Led by NIST the strategy sets forth NICE's vision, mission, values, and a set of goals and objectives. *DHS, DOC, DoD, DOE/SC, DOL, ED, FCC, NIST, NSA, NSC, NSF, ODNI, OPM*
- **NICE Interagency Coordinating Council:** Convene Federal Government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development. The meetings will provide an opportunity for the NICE Program Office, located at NIST, to communicate program updates with key partners in the Federal Government and to learn about other Federal Government activities in support of NICE. The group will also identify and discuss policy issues and provide input into the strategic direction for NICE. *DHS, DOC, DoD, DOE/SC, DOL, ED, FCC, NIST, NSA, NSC, NSF, ODNI, OPM*
- **Workforce cybersecurity education and training provisions of the Cybersecurity Executive Order:** The *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (13800) dated May 11, 2017, directed the Secretary of Commerce and the Secretary of Homeland Security to (1) assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future; and (2) provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in the public and private sectors. This effort is proceeding. *DHS, DOC*

Enabling R&D for High-Capability Computing Systems (EHCS) PCA

EHCS involves R&D to advance high-capability computing and develop fundamentally new approaches in high-capability computing, including R&D in hardware and hardware subsystems, software, architectures, system performance, computational algorithms, data analytics, development tools, and software methods for extreme data- and compute-intensive workloads.

The High End Computing IWG reports its relevant activities under the EHCS PCA.

High End Computing (HEC) IWG

***Participating Agencies*: Air Force, Army, DARPA, DOE/NNSA, DOE/SC, EPA, IARPA, NASA, NIH, NIST, NSA, NSF, OSD**

The HEC IWG coordinates Federal R&D of innovative future computing technologies and supercomputers to extend U.S. leadership in advanced computing in support of the Nation's priorities such as economic competitiveness, national security, and U.S. leadership in science, engineering, and technology. Advances in high-capability computing systems (HCS) technologies impact the entire spectrum of computing devices, from the largest system to handheld devices, as well as emerging industries and opportunities such as precision medicine, smart and connected communities, and the next wave of autonomous machines.

Strategic Priorities

- **Extreme-scale computation:** Develop algorithms, software, and hardware technology supporting data and compute-intensive scientific applications for exascale computers; explore novel approaches for data-intensive, high-capability computing; and pursue research to increase performance.
- **New directions in HCS hardware, software, computer science, and system architecture:** Develop "beyond Moore's Law" scientific frameworks and architectures, memory, programming environments, measurement science, thermal management, and hardware and software prototypes; and advance R&D in quantum, neuromorphic, and superconducting computing.
- **Productivity and broadening impact:** Develop benchmarks for new architectures, frameworks to lower design barriers, and common tools for computational modeling and simulation and analysis of data; and conduct crosscutting activities, including expanding the HCS workforce.

Key Programs

- **Extreme-scale computation:**
  - Support the Cyber Hardened Embedded and Exascale Trusted Architecture program for scalable, low-latency, high-throughput, energy-efficient, data-intensive HCS. *AFRL, OSD*
  - Explore HCS, data-intensive HCS, and machine learning. *HPCMP*
  - Continue work on the Exascale Computing Project, including the PathForward program, to ensure that node and system designs meet exascale goals. *DOE/NNSA, DOE/SC*
  - Develop data management, analysis, and visualization techniques and partnerships. *DOE/SC*
  - Develop novel software methods for extreme-data and compute-intensive workloads. *EPA*
  - Enhance software engineering efforts for extreme-scale parallelism. *NASA*
  - Develop new extreme-scale computational approaches for biomedical simulations. *NIH*
  - Research security and privacy requirements, capabilities, and controls for HCS. *NIST*
  - Support the Scalable Parallelism in the Extreme, Foundational Microarchitecture Research, and Computational and Data-Enabled Science and Engineering programs. *NSF*

- **New directions in HCS hardware, software, computer science, and system architecture:**
  - Develop scalable multi-layer silicon photonic interconnects with all-optical switching and all-optical networking hardware and architecture. *AFRL, OSD*
  - Research and evaluate prototypes exploring technologies beyond Moore's Law, including quantum testbeds and quantum information science. *DOE/SC*
  - Continue the programs in quantum computing and the Cryogenic Computing Complexity and Machine Intelligence from Cortical Networks program. *IARPA*
  - Continue work on quantum computing through partnership with industry. *NASA*
  - Continue research on quantum information science, including quantum algorithms and complexity, post-quantum cryptography, and specialized quantum devices. *NIST*
  - Research probabilistic and neuromorphic computing, and research memory improvements through exploration of 3D stacks and novel materials. *NSA*
  - Support the Ideas Lab and Practical Fully Connected Quantum Computer Challenge, and explore quantum applications through the Quantum Information Science program. *NSF*
- **Productivity and broadening impact:**
  - Advance the U.S. workforce through internships, technology transfer, and training. *HPCMP*
  - Support the Computational Science Graduate Fellowship. *DOE/SC*
  - Build the HCS workforce through summer school, internships, and fellowship programs. *NASA*
  - Develop methods for quantifying reproducibility and uncertainty in scientific computing, and develop algorithms and software innovations to process extreme data. *NIST*
  - Develop machine-learning and deep-learning benchmarks, and build the HCS workforce. *NSA*

Key Coordination Activities

- **Extreme-scale computation:**
  - Explore HCS and Big Data coherence to ensure support for emerging data-intensive applications and domains. *HEC IWG agencies, Big Data IWG agencies*
  - Continue collaboration among Federal agencies for broad use and applicability of exascale computing. *HEC IWG agencies, other agencies*
- **New directions in HCS hardware, software, computer science, and system architectures:**
  - Explore supercomputing in the cloud to determine applicability and efficiencies for a subset of Federal HCS needs. *DoD, DOE/SC, NASA, NIH, NSF*
  - Research computer memory improvements and machine learning. *DOE/NNSA, DOE/SC, IARPA, NIST, NSA*
  - Explore other "Beyond Moore's Law" computing research. *HEC IWG agencies*
- **Productivity and broadening impact:**
  - Collaborate to develop benchmarks, performance test cases, and HCS application metrics. *HEC IWG agencies*
  - Facilitate access to and sharing of knowledge gained and lessons learned from HCS hardware and software R&D. *HEC IWG agencies*
  - Support the National Strategic Computing Initiative. *HEC IWG agencies, other agencies*
  - Support workforce development through the Quantum Science Summer School. *DOE/SC, NSF*

High-Capability Computing Infrastructure and Applications (HCIA) PCA

HCIA involves operation and utilization of systems and infrastructure for high-capability computing. This includes computation- and data-intensive systems and applications, directly associated software, communications, storage, and data management infrastructure, and other resources supporting high-capability computing.

The High End Computing IWG reports its relevant activities under the HCIA PCA.

High End Computing (HEC) IWG

***Participating Agencies*: Army, DOE/SC, EPA, NASA, NIH, NIST, NOAA, NSF**

The HEC IWG focuses on coordination of high-capability computing infrastructure and applications, including its modernization. HCIA provides tens of billions of computing hours on the Nation's most powerful computing platforms, as well as software and expertise to enable researchers from academia, government, and industry to pursue high-fidelity analysis for advanced weapons and nuclear stockpile stewardship, early-stage research of advanced technologies, detection and treatment of diseases, and many other applications of national interest.

Strategic Priorities

- **Leadership-class and production high-capability computing systems:** Provide the increasingly capable HCS needed to meet critical national needs; provide smaller HCS clusters for research and education across all of science and engineering; and reduce the energy requirements and environmental impact of computing technology at all scales.
- **Advancement of HCS applications:** Develop algorithms and applications software for current and next-generation HCS platforms to preserve the performance of existing codes.
- **HCS infrastructure:** Provide diverse user communities with efficient, effective, and dependable access to HCS facilities and resources, including testbeds, communications, storage, software tools, and applications and system support; and enhance existing infrastructure capabilities for computational and data-enabled science, modeling, simulation, and analysis.
- **Productivity and broadening impact:** Share lessons learned and best practices for acquisition and enhancement of HCS resources; reduce total ownership costs of HCS; integrate resources for improved productivity; design and develop collaborative work environments for high-capability simulation and data analytics through high-speed networks and advanced data storage and management; and pursue cross-cutting activities, including developing the next-generation computational workforce.

Key Programs

- **Leadership-class and production high-capability computing systems:**
  - Provide large-capacity, high-capability HCS to DoD; provide shared, above-secret capabilities to address critical DoD mission requirements. *HPCMP*
  - Provide large-capacity HCS at the National Energy Research Scientific Computing Center, and update and provide large-capability leadership-class systems at the Argonne and Oak Ridge Leadership Computing Facilities. *DOE/SC*
  - Provide data-intensive systems for mission-related research. *EPA*
  - Increase HCS capacity using modular computing technology for energy efficiency. *NASA*
  - Operate internal and external HCS systems of diverse leading-edge architecture. *NOAA*
  - Operate and support HCS through the Leadership-Class Computing program; a diverse set of mid-tier HCS resources through the Innovative HPC Acquisition program; petascale

computing resources through the National Center for Atmospheric Research/Wyoming Supercomputing Center program; and local campus HCS clusters through the Major Research Instrumentation program. *NSF*

- **Advancement of HCS applications:**
  - Develop DoD multiphysics software applications to maintain military superiority. *HPCMP*
  - Continue research on applied mathematics and algorithms, and initiate activity in machine learning to optimize output from data-intensive programs. *DOE/SC*
  - Develop the analytics, algorithms, and computational science required for research. *EPA*
  - Support multiscale modeling of biomedical processes for improved disease treatment. *NIH*
  - Prepare NOAA's software suite for next-generation architectures. *NOAA*
  - Develop parallel algorithms, large-scale high-performance image processing techniques, and computation methods required for applications in measurement science. *NIST*
- **HCS infrastructure:**
  - Provide computational tools and techniques, data analysis and visualization tools, application support, and HCS system expertise. *HPCMP*
  - Support HCS and data analysis; continue Energy Sciences Network upgrades. *DOE/SC*
  - Provide HCS and associated software, communications, tools, and data management infrastructure. *EPA*
  - Partner with HCS cloud providers for data processing, analytics, and burst HCS usage. *NASA*
  - Provide shared interoperable cloud computing environment, high-capacity infrastructure, and computational analysis tools for high-throughput biomedical research. *NIH*
  - Support systems integration for the R&D HCS systems. *NOAA*
  - Support shared user service and HCS, storage, visualization, and data services. *NSF*
- **Productivity and broadening impact:**
  - Continue support for the National Energy Research Scientific Computing Center and the Oak Ridge and Argonne Leadership Computing Facilities, including training, application readiness, and outreach to prepare the scientific community for future system upgrades. *DOE/SC*
  - Provide science gateways, and continue support for education, training, and outreach to increase the competencies and diversity of the current and next-generation workforce. *NSF*

Key Coordination Activities

- **Leadership-class and production HCS systems, and advancement of HCS applications:**
  - Coordination of access to leadership HCS for the Nation's broad R&D community. *DOE/SC, HPCMP, NASA, NOAA, NSF*
  - DOE intra-agency collaboration for joint execution of ECP. *DOE/NNSA, DOE/SC*
  - Provision of HCS compute core hours for HCS applications. *HEC IWG and other agencies*
- **High-capability computing systems infrastructure:**
  - Multiagency collaboration on the Remote Sensing Information Gateway. *EPA, NASA, NOAA*
- **Productivity and broadening impact:**
  - Interagency participation in annual proposal review panels and PI meetings. *HEC IWG agencies*
  - Education/workforce development through support for the Federal HCS inventory portal for learning, workforce development, and HCS resources available to the public. *HEC IWG agencies*
  - Transfer of computational skills and technologies to partners in industry and academia. *HEC IWG agencies*

Intelligent Robotics and Autonomous Systems (IRAS) PCA

IRAS involves R&D of intelligent robotic systems, including R&D in robotics hardware and software design and application, machine perception, cognition and adaptation, mobility and manipulation, human-robot interaction, distributed and networked robotics, and increasingly autonomous systems.

The Intelligent Robotics and Autonomous Systems IWG reports its activities under the IRAS PCA.

Intelligent Robotics and Autonomous Systems (IRAS) IWG

***Participating Agencies*: Air Force, Army, DOE/EM, DOT, NASA, Navy, NIFA, NIH, NIJ, NIOSH, NIST, NSA, NSF, OSD**

The IRAS IWG coordinates R&D in the areas of autonomous robots and other intelligent physical systems, such as smart grids and surveillance drones. IRAS is concerned with developing robust, safe, and ethical robots and intelligent systems that can assist people in their work and everyday lives. This important work develops collaborative robots in factories, assistive devices for the elderly and disabled, systems to monitor and maintain national resources and infrastructure, and systems to support national security and defense.

Strategic Priorities

- **Effective human-robot collaboration:** Further natural human-robot communication and safe human-robot physical interaction to increase quality of work and life. Assist those with developmental or acquired disabilities to maximize independence.
- **Advanced robotic and autonomous systems:** Develop and validate metrics, test methods, information models, protocols, and tools to advance robot system performance and safety, and develop measurement science infrastructure to specify and evaluate the capabilities of remotely operated or autonomous aerial, ground/underground, and aquatic robotic systems.
- **Intelligent physical systems**: Develop smart and autonomous systems that robustly sense, plan, act, learn, and behave ethically in the face of complex and uncertain environments.
- **Wearable robotic fabrics and devices:** Develop and deploy human-worn and human-attachable robotic fabrics and devices to enhance warfighter safety and increase performance and tactical edge in combat.

Key Programs

- **Alliance Partnership:** Build expertise in robotics, produce guidance for safe interaction of humans and robots, and identify research needs. *NIOSH, OSHA, industry partners*
- **National Robotics Initiative 2.0 (NRI 2.0):** Integrate ubiquitous and collaborative robots that work seamlessly with people to assist in every aspect of life. *DoD, DOE/EM, NASA, NSF, OSD, USDA*
- **Smart and Autonomous Systems (S&AS):** Pioneer intelligent physical systems that robustly think, act, learn, and behave ethically. *NSF, industry partners*
- **Robust Intelligence:** Develop intelligent systems that operate in complex, realistic contexts. *DoD, NSF, OSD*
- **Mind, Machine, and Motor Nexus:** Support research towards an integrated treatment of human intent, perception, and behavior in interaction with embodied and intelligent engineered systems and as mediated by motor manipulation. *DoD, NSF*
- **Dynamics, Control, and Systems Diagnostics**: Advance fundamental research on the analysis, measurement, monitoring, and control of dynamic systems. *NSF*

- **Energy, Power, Control, and Networks:** Invest in systems and control methods for analysis and design of CPS to ensure stability, performance, robustness, and security. *DoD, NSF*
- **Continuum, Compliant, and Configurable Soft Robotics:** Support interdisciplinary research to fill fundamental gaps in the understanding of soft robots characterized by continuum structures with highly compliant materials or components. *AFOSR, DoD, NSF*
- **Robotic Systems for Smart Manufacturing:** Advance measurement science to improve robotic system performance, collaboration, agility, and ease of integration into the enterprise to achieve dynamic production for assembly-centric manufacturing. *NIST*
- **Emergency response and homeland security robots:** Develop the measurement science and standards infrastructure to evaluate the capabilities of remotely operated robotic systems, including autonomous functionalities and operator proficiency. *DoD, NIST, OSD*
- **Surgical Tools, Techniques, and Systems:** Research and develop next-generation tools, technologies, and systems to improve the outcomes of surgical interventions. *NIH*
- **Mathematical Modeling, Simulation, and Analysis:** Support development of simulation technology for training and education in clinical practice and biomedical research; simulation algorithms for understanding and prediction of health and disease; and simulations designed to reduce medical errors and increase human safety. *DoD, NIH*
- **Rehabilitation Engineering, Devices, and Technology Development:** Develop systems that can enhance an individual's mobility, communication, hearing, vision, and cognition. *DoD, NIH*
- **Autonomous resupply/logistic systems:** Accelerate, demonstrate, and evaluate the effective use of autonomous systems for coalition-based assured autonomous resupply for military logistics. *Army, OSD*
- **Visual common sense:** Develop machines that acquire visual common sense; represent visual knowledge in compositional models with contextual relations; and advance understanding of scenes through reasoning about geometry, functions, physics, intents, and causality. *ONR*

Key Coordination Activities

- **NRI 2.0:** Annual PI Review on ubiquitous and collaborative robots. *DoD, DOE/EM, NASA, NSF, USDA*
- **S&AS:** Annual PI Review Meeting on intelligent physical systems that robustly think, act, learn, and behave ethically. *NSF, industry partners*
- **Performance standards for response robots** in homeland security applications. *DoD, DOJ, DOS, NIST*
- **Modeling and simulation in robotics:** IRAS workshop connecting roboticists and researchers in modeling and simulation to advance the use of simulation in planning, control, and learning. *DOE/EM, DOT, NASA, NIFA, NIH, NIJ, NIOSH, NIST, NSA, NSF, OSD*
- **Exoskeleton and exosuit standards development:** Ongoing participation in ASTM Committee F48 on Exoskeletons and Exosuits, which works to develop consensus standards for security, safety, quality, performance, ergonomics, terminology, and integration for systems and components throughout their life cycles for numerous military, medical, and consumer applications. *DoD, DOE/EM, NIST, NIH, NIOSH, NRC, OSHA*
- **Robots in manufacturing:** Technical advice and input to the DoD Advanced Robots for Manufacturing Institute. *DoD, NIST*
- **Verification of autonomous systems working group.** *NIST, NRL, ONR*

Large Scale Data Management and Analysis (LSDMA) PCA

LSDMA involves R&D to extract knowledge and insight from data, including R&D in the capture, curation, management, access, analysis, and presentation of large, diverse, often multisource, data.

The Big Data IWG reports its activities under the LSDMA PCA.

Big Data IWG

***Participating Agencies*: DARPA, DHS, DOE/NNSA, DOE/SC, EPA, NARA, NASA, NIH, NIST, NOAA, NSA, NSF, OSD, USAID, USGS**

The Big Data IWG coordinates Federal R&D to enable effective analysis, decision-making, and discoveries based upon large, diverse, and real-time data. Expanding capabilities to collect, store, and access big data will accelerate scientific discovery and innovation, lead to new fields of research and areas of inquiry, and provide vast resources to enhance national security, build individualized educational programs, and create new capabilities that support economic growth and novel solutions to pressing societal issues.

Strategic Priorities

- **Effective use of large-scale data resources:** The overarching goal is low-latency analytics that empower confident, data-driven discovery and decision-making regardless of infrastructure, technology, or data source, while also addressing issues of privacy and resiliency.
- **Measurement and benchmarking:** Increasingly complex data and data analytics methods require new measurement and benchmarking capabilities to assure trustworthiness and usability while also moving users from correlation-based analysis to causal modeling.
- **Interoperability of diverse data types and sources:** This focus area aims to further improve accessibility, transparency, and accountability.
- **Workforce development:** These efforts address the shortage of data science expertise necessary to move big data projects forward.

Key Programs

- **Foundational research:** Discover new tools and methodologies to use the massive amount of data and information that is available to solve difficult problems. DARPA programs address problems related to generating alternative hypotheses from multisource data, machine reading and automated knowledge extraction, low-resource language processing, media integrity, automated software generation and maintenance, scientific discovery and engineering design in complex application domains, and modeling of global-scale phenomena. NSF will invest in the Harnessing the Data Revolution for 21st-Century Science and Engineering (HDR) Big Idea, which includes Transdisciplinary Research in the Principles of Data Science, as well as on "Foundation" research in its BIGDATA research program. *DARPA, NSF*
- **Development of infrastructures and tools:** Enable interoperability and usability of data to allow users to access diverse data sets that interoperate both within a particular domain and across domains. This effort involves building teams, infrastructure components, and governance models (i.e., frameworks and standards) to reconcile data and allow it to "mash up" regardless of the data source and structure. The NIH Data Translator and the multi-agency engagement in the Open Knowledge Network are examples. *DARPA, NARA, NIH, NIST, NSF*
- **Real-time analytics:** Invest in technologies to reduce the time delay between data intake and analysis and decision making. For example, DHS is investing in analytical frameworks to address

data latency, compromise, and failure in networks that support first responders. *DARPA, DHS, NIH, NIST, NSF*

- **Data governance and testing:** Develop data science measurement and benchmarking capabilities of complex data and data analytics methods to improve the reliability, robustness, accuracy, access, generalizability, usability, and performance of solutions for data-driven discovery and decision making. Examples include NIST's standards and measurements for Data Science Evaluations and NARA's testbed investigations related to records management. *DHS, NARA, NIH, NIST, NSF*
- **Transition to practice:** Target effective technology development and translate advances in applied research into operational tools and technologies. Examples include developing screening tools for U.S. Citizenship and Immigration Services and U.S. Customs and Border Protection, and big data analytics for the Federal Emergency Management Agency and U.S. Immigration and Customs Enforcement. *NARA, NIH, NIST*
- **Workforce development:** Develop innovative data science research and training opportunities that build workforce capacity, strengthen teams, and rapidly advance science. *NIH, NSF*

Key Coordination Activities

- **NIST Big Data Public Working Group:** Develop consensus on important fundamental concepts related to Big Data such as definitions, taxonomies, secure reference architectures, and a technology roadmap. *Army, DISA, Interior, NASA, NARA, NIST, NSF, VA*
- **Big Data Hubs:** Leverage expertise and build regional public-private partnerships to solve regional data science problems in both the public and private sectors. *DHS, NSF*
- **Real-time Analytics for Multi-Latency, Multi-party, Metro-scale Networks:** Examine data latency issues in large-scale networks. *DHS, NSF*
- **HDR Big Idea:** Focus on (1) research in three thematic areas: foundations of data science, data science systems and algorithms, and data-intensive applications across science and engineering domains; (2) development of advanced cyberinfrastructure to support research in data-intensive science and engineering; and (3) education and training in data science. *NIH, NSF*
- **NIH Data Commons Pilot:** Leverage expertise in data science, computer science, and information technology, and with help from cloud service providers and biomedical researchers, focus on high-value biomedical data sets with an ultimate goal of interoperability with existing data structures such as the National Cancer Institute Genome Data Commons and the American Heart Association Precision Medicine platform. *NIH*
- **DARPA Low Resource Languages for Emergent Incidents (LORELEI) program**: Develop human language technology for low-resource foreign languages: LORELEI technology specifically aims to provide situational awareness by identifying key elements of information such as names, events, sentiment, relationships, and locations. LORELEI technology development is being coordinated with U.S. military and civilian humanitarian assistance and disaster relief activities. *DARPA*

Large Scale Networking (LSN) PCA

LSN involves R&D of networking technologies and services, including R&D in networking architectures, wireless networks, software-defined networks, heterogeneous multimedia networks, testbeds, grid and cloud research and infrastructure, network services and cloud computing middleware, identity management, and end-to-end performance enhancement and performance measurement.

The following groups report their activities under the LSN PCA:

- Large Scale Networking IWG, including the Broadband Research and Development Group, Joint Engineering Team, and Middleware and Grid Interagency Coordination Team
- Wireless Spectrum Research and Development IWG

Large Scale Networking (LSN) IWG

***Participating Agencies*: Air Force, Army, ARS, DARPA, DOE/SC, DREN, FAA, FCC, IARPA, NASA, Navy, NIH, NIJ, NIST, NOAA, NSA, NSF, OSD, USGS**

The LSN IWG coordinates Federal R&D in networking technologies and services—including network architectures, wired and wireless network infrastructures, grid and cloud middleware research, and communication protocols—enabling the robust transfer of data from ground, sea, air, and space systems to support national security, commercial industry, and scientific research.

Strategic Priorities

- **Future networks:** Develop concepts, techniques, architectures, and protocols for future networks, including heterogeneous, smart, self-managed, hybrid, peer-to-peer networks.
- **Cloud infrastructure enhancements:** Develop a common approach for Infrastructure as a Service, including best practices for common reference virtualization platforms.
- **Enhanced network architecture for data analytics:** Develop next-generation network architecture capabilities in highly distributed environments for large-scale global data flows.
- **Network security and resiliency:** Develop, evaluate, and standardize technologies to achieve security and resilience in emerging wireless networks and multidomain internets and to protect core network infrastructure, focusing on critical infrastructure protection, the emerging IoT, satellite and advanced wireless networks, and cyber defense at scale.
- **Wireless networks:** Develop technology, standards, testbeds, and tools to enable improved interconnectivity, high-bandwidth mobile wireless networks, and increased mobile network architecture capacity.

Key Programs

- **Develop concepts, techniques, architectures, and protocols for future networks**:
  - New software-defined-network (SDN) architectures and demonstrations. *DOE/SC, DREN, NASA, NIST, NSA, NSF*
  - High-speed data links. *DOE/SC*
  - Next-generation network research and testing. *DOE/SC, DREN, NIST, NSF*
  - Deterministic networking for integrated fires. *Navy*
  - Future Internet technologies for the IoT. *NIST*
  - Programmable, high-performance measurement technologies for SDN. *NIST*
  - Transition to practice and critical infrastructure. *DOE/SC, NSF*
- **Develop cloud infrastructure enhancements**:
  - SDN and software-defined Internet exchange and perimeter (SDX/SDP) application testing and demonstrations. *DOE/SC, DREN, NASA, NIST, NSA, NSF*

  - Cloud computing standards, network function virtualization, SDN technologies. *DOE/SC*, *NIST*
  - Network technology and systems R&D, new hardware for future cloud, and reproducibility of research on cloud systems. *DOE/SC*, *NSF*
  - Innovative network transport and cloud connection services. *DOE/SC, DREN, NOAA*
  - Cloud computing architectures. *DOE/SC*
  - Critical infrastructure. *AFRL*
- **Develop enhanced network architecture for data analytics:**
  - Couple big data sources with near-real-time data analytics, and accelerate commercialization of 100 Gbps networking technologies. *DOE/SC*
  - Enhance efficiency of big data transfers over high-bandwidth connections. *DOE/SC, DREN*
  - Promote cooperation and test beds for large data transfers and new architectures. *DOE/SC*
  - Translate research to end-to-end applications. *DOE/SC*, *NSF*
  - Address large data flows in trusted Internet connection (TIC) environments. *NASA*
  - Address data analytics at scale. *DOE/SC*, *NSA*
  - Deliver next-generation supercomputing support for advanced analytic modeling. *DOE/SC*, *NOAA*
  - Pursue applications in precision medicine, mobile health, telemedicine, and adaptive networks for data and image processing. *DOE/SC*, *NIH*
- **Develop and standardize technologies to enhance network security and resiliency:**
  - Pursue resilient communications and multi-level security routing. *AFRL*
  - Advance cyber situational awareness. *AFRL, CERDEC*
  - Enhance monitoring/intrusion detection mechanisms. *DOE/SC, NASA*
  - Enhance cybersecurity capabilities, including SDN and/or network function virtualization. *DREN, NASA, NIST*
  - Develop trustworthy network infrastructure. *DOE/SC*, *NSF, NIST*
  - Develop protected satellite communications. *Navy*
  - Advance cyber defense at scale. *NSA*
  - Research cyber-infrastructure protection. *NSF*
  - Address novel security architectures for IoT, Internet infrastructure protection, and networked cyber-physical systems. *NIST*
- **Develop technology, standards, testbeds, and tools to improve wireless networks**:
  - Directional networking and cyber-electromagnetic activities. *CERDEC*
  - Multilevel information sharing across tactical wireless networks. *DARPA*
  - Wideband, digital beam forming. *Navy*
  - Machine-to-machine communication networks. *NIST*
  - Beyond-5G wireless technologies supporting scalable experimentation. *NSF*

Key Coordination Activities

- **Software defined technologies and demonstrations:** SDN/SDX/SDP applications testing and demonstrations; tactical-edge SDN collaboration; and complex systems experimental design. *ARL, DoD (e.g., CERDEC), DOE/SC, DREN, NASA, NIST, NSA, NSF*
- **DoD interservice collaboration:** Command, control, communications, and information systems, and cyber communities of interest. *AFRL, ARL, CERDEC, DARPA, Navy, OSD*
- **Health network**: Multiagency neuroscience research collaborations, including on novel neuro-technologies and lab technologies and smart and connected health. *FDA, IARPA, NIH, NSF, Industry*
- **Networking for disaster recovery and crisis management:** Expansion and promulgation of Disaster Information Management Research Center resources. *National Library of Medicine, NIH*

- **National/transoceanic 100 Gbps connectivity:** International Research Network Connections program support for high-performance network connectivity necessary for international science and engineering research and education collaborations**.** *DOE/SC, DREN, NASA, NSF, NOAA*
- **Wireless networks:**
  - Secure Handhelds on Assured Resilient networks at the tactical Edge program: Information sharing across tactical wireless networks. *Army, DARPA, SOCOM, USMC*
  - Small satellite communications. *AFRL, CERDEC, Navy*
- **Broadband Research and Development Group:** Interagency collaboration and focus on addressing disparities in nationwide broadband access, adoption, and usage. *Census, DARPA, DHS, DOE/SC, DOL, ED, FCC, HRSA, NIH, NIJ, NIST, NOAA, NSF, NTIA, OSD, USDA*
- **Joint Engineering Team:** Coordination on networking, advanced technologies, end-user requirements, science user interfaces, and research and storage networks; end-to-end big data transport and application testbeds; TICs and TIC access providers; interdomain, end-to-end metrics; and tool sharing. *DOE/SC, DREN, FCC, NASA, NIH, NIST, NOAA, NSA, NSF*
- **Middleware and Grid Interagency Coordination Team:** Coordination on identity management, distributed computing, middleware, and cloud and grid computing services and information exchanges; cloud and grid standards and implementation; best practices for resource architecture, access, and management; and security and privacy. *DOE/SC, FCC, NIST, NSF*

Wireless Spectrum R&D (WSRD) IWG

***Participating Agencies*: Air Force, Army, DARPA, DHS, FAA, FCC, NASA, Navy, NIJ, NIST, NOAA, NSF, NTIA, OSD**

The WSRD IWG coordinates spectrum-related R&D activities across the Federal Government to facilitate efficient, effective investment in spectrum sharing technologies and systems. It engages with academia, the private sector, and international public R&D agencies.

Strategic Priorities

- **Spectrum utilization:** Develop technologies and methodologies that will increase spectrum efficiency, flexibility, and adaptability.
- **Device adaptation:** Provide capabilities needed for devices to monitor their environments and adapt in real time to acquire spectrum resources to perform specific tasks, from conveying delicate science/weather measurements to coordinating in-flight communications during an attack.
- **Higher frequency utilization:** Expand the Nation's communications capacity by using higher-frequency bands (>20 GHz) and optical links.

Key Programs

- **Accelerating technology to market:**
  - National Advanced Spectrum and Communications Test Network: Provide a neutral forum for addressing spectrum-sharing challenges. *DOD, NIST, NTIA*
- **Next-generation wireless research:**
  - Platforms for Advanced Wireless Research: Enable experimentation of robust new wireless devices, communication techniques, networks, systems, and services. *NSF*
  - Develop communications for unmanned aerial vehicle swarms. *AFRL, NRL*
  - Higher-frequency (>20 GHz) and free-space optical communications: Research technologies to augment other communication capabilities. *AFRL, NASA, NRL, NSF*

- **Dynamic spectrum access and spectrum diversity:**
  - Spectrum Efficiency, Energy Efficiency, and Security: Support communications and networking systems in efficient and dynamic spectrum environments. *NSF, NTIA*
  - Aerial Layer Networking**:** Build spectrum agility and resilience for heterogeneous users. *AFRL*
  - Shared Spectrum Access for Radar and Communications and Enhancing Co-existence for Force Protection. *CERDEC, DARPA, NTIA*
  - Science sensor radio frequency interference mitigation and sharing: Enable weather/science sensor observations in noisy frequency bands, and spectrum sharing. *NASA, NOAA, NSF, NTIA*
- **Robust, secure, and dependable systems and networks:**
  - Next-generation aerial directional data link and networking: Research methods to increase interference tolerance, spectral efficiency, and frequency reuse. *AFRL*
  - Electromagnetic Maneuver Command and Control: Develop technologies to coordinate and optimize radio system functionality. *NRL*
- **Dynamic spectrum planning and management—situational awareness, modeling, simulation:**
  - RadioMap: Enable efficient spectrum use by providing an accurate picture of real-time radio spectrum use across frequency and geography in complex radio environments. *DARPA*
  - Dynamic Radio Frequency Route Management: Provide access to all available communications links to enable the highest level of communications throughput. *NRL*
  - SpecMon: Achieve ubiquitous, networked, and standardized radio frequency sensing and data distribution for automated spectrum enforcement. *NTIA*
  - IPC Methods**:** Standardize receiver models and associated interference protection criteria to support automation of spectrum management. *NTIA*
  - Production-level software: Release packages that execute advanced and data-driven radio wave propagation models to support spectrum management. *NTIA*
  - Spectrum sharing metrology: Do statistical modeling of aggregate interference, algorithms, spectrum occupancy metrics, and measurement methodologies for detection and protection of incumbents, and testing and validation methods of spectrum sharing systems. *NIST*
- **Multivendor, multisystem integration:**
  - Network C2: Enable multivendor, multiplatform radio enclaves via an agnostic monitoring and messaging protocol. *AFRL*
  - Foster nationwide interoperability and advanced communications technology for the Nation's public safety community. *DEA, DHS, NIST, NTIA*
  - Next-generation Software Defined Radio Frequency: Enable a broad range of selectable frequency bands, channelization, and use of numerous communications links. *AFRL*

Key Coordination Activities

- **Interdepartmental Radio Advisory Committee:** Assist in assigning frequencies to Federal users and in developing and executing related policies, programs, procedures, and technical criteria. *NASA, NSF*, *NTIA, and 17 other agencies*
- **Future Generation Wireless Roadmap Working Group:** Forecast the evolution of communications technology over the next 20+ years. *DARPA, NIST*
- **Millimeter-wave Channel Modeling Alliance:** Provide a nexus for global efforts to define the future radio channels through which next-generation 5G wireless will operate. *NIST, NSF*, *NTIA*
- **National Advanced Spectrum and Communications Test Network:** Organize a national network of Federal, academic, and commercial test facilities to provide the testing, modeling, and analysis necessary to develop and deploy spectrum-sharing technologies and inform future spectrum policy and regulations. *DOD, NIST*, *NTIA*

Software Productivity, Sustainability, and Quality (SPSQ) PCA

SPSQ involves R&D to advance timely and affordable development and sustainment of quality software, including R&D to significantly improve software production processes, productivity, quality, economics, sustainability, measurement, assurance, and adaptability.

The Software Productivity, Sustainability, and Quality IWG reports its activities under the SPSQ PCA.

Software Productivity, Sustainability, and Quality (SPSQ) IWG

Participating Agencies: **Air Force, BLS, FDA, IARPA, NASA, Navy, NIH, NIJ, NIST, NOAA, NRC, NSA, NSF, ONR, OSD**

The SPSQ IWG coordinates Federal R&D to achieve orders-of-magnitude reduction in software defects and in the time and cost of developing and sustaining software. With the U.S. Government, economy, and military depending on increasingly complex computer software, new software development technology is essential to promoting U.S. innovation and competitiveness, contributing to American prosperity, military superiority, energy dominance, security, and health.

Strategic Priorities

- **Advance discovery and innovation** through the development and sustainment of low defect, low vulnerability software, and the productivity of software engineering, including:
  - Foundational research on software science and engineering.
  - Next-generation software development and sustainment concepts, methods, and tools.
  - Interdisciplinary, system-oriented approaches that lead to transformational concepts.
  - Capabilities to build evolvable, sustainable, long-lived software-intensive systems.
- **Improve critical software** by increasing execution efficiency, reducing vulnerability to attack, and increasing security against leaking sensitive information.
- **Provide trust and resilience in software** to enable it to fight through and recover from attacks in real time.
- **Reduce software vulnerabilities** through the development of effective, economic solutions.
- **Modernize and manage research and regulatory infrastructures** to improve the safety and security of digital systems.
- **Support software-related STEM education and training** to develop the future workforce.

Key Programs

- **Software and Hardware Foundations Program:** Develop scientific and engineering principles and new logics, languages, architectures, and tools for specifying, designing, programming, analyzing, and verifying software and software-intensive systems; formal methods; verification and validation tools for development of assured trustworthy software; formal definitions of weaknesses; standards for certification; and techniques that enable prediction of cost and schedule for large-scale software projects. *AFRL, NASA, NIST, NOAA, NSF, ONR, OSD*
- **Computer Assisted Programming for Heterogeneous Architectures:** Conduct research with industry to enable efficient conversion of software across different hardware architectures, especially in high-performance computers, applying computer science ideas (e.g., program synthesis and machine learning) for mapping software to new hardware targets. Ultimately, this research can reduce the need for highly specialized expertise. *NSF, industry partners*
- **Formal Methods in the Field:** Develop rigorous and reproducible methods for designing and implementing correct-by-construction systems and applications with provable guarantees

through joint research projects between formal methods researchers and researchers in other areas of computer science and engineering. Current focus areas for research are in computer networks, cyber-human systems, machine learning, and operating/distributed systems. *NSF*

- **Total Platform Cyber Protection:** Investigate tools to reduce software vulnerabilities and improve execution efficiency by removing unnecessary code from preexisting software automatically (as well as with user selection). *ONR*
- **Secure and Trustworthy Cyberspace:** Increase software security through research on security engineering; software analysis/synthesis to detect and protect programmed and networked cyberspace; and the application of formal methods and programming language approaches. Current focus areas include mobile applications, language-based security, binaries, and operating systems. *NSF*
- **BRAIN Initiative:** Support R&D to develop and test sustainable, high-quality software technologies that will enable new ways to model, analyze, treat, cure, or prevent brain disorders through better understanding of the human brain. *FDA, IARPA, NIH, NSF*
- **All of Us Initiative:** Leverage R&D to develop and sustain high-quality software technologies to enable researchers to make connections between the environment and the genomes of individuals in a 1 million+ cohort of volunteers. *NIH, NIST, other SPSQ IWG agencies*
- **NIH Data Commons pilots:** Develop the software technology and formalisms to enable a shared, interoperable, and sustainable computing environment that takes advantage of efficient cloud computing platforms to facilitate access and catalyze the sharing, use, reuse, interoperability, and discoverability of shared digital research objects with assurance. *NIH*
- **Software Assurance Reference Dataset:** Provide hundreds of thousands of programs with known security flaws to the software engineering community, including U.S. industry, to assess and refine tools. *DARPA, IARPA, NIST, NSA, other Federal and private sector partners*
- **Software Assurance Marketplace:** Provide a national marketplace of continuous software assurance capabilities for researchers and developers to help reduce the number of vulnerabilities deployed in new software systems. *AFRL*
- **Agile Resilient Embedded Systems:** Augment demonstration of self-patching systems (e.g., in the Cyber Grand Challenge) with the improved verification that scale-up requires. *AFRL*

Key Coordination Activities

- **Application of Category Theory to systems engineering problems:** Collaboration with federally funded research at universities to provide interoperability among multiscale, multidomain, and heterogeneous tools and data. *NIST, NSF, NASA, other SPSQ IWG agencies*
- **Software verification and validation:** Collaboration to develop effective approaches for next-generation air transportation and related concepts, modeling, and simulation tools. *AFRL, DOD Service research organizations, NASA, ONR, OSD*
- **Health IT R&D:** Coordination with the HITRD IWG to support Federal R&D for software-intensive systems and testing tools (e.g., medical device interoperability, HL7 Validation Tool), software implementations (e.g., electronic health records, AI/ML algorithms), and the impact on health outcomes of low-defect, low-vulnerability medical software. *FDA, NIH, NIST, NSF*
- **Software and Supply Chain Assurance Forum:** An ongoing public-private sector initiative to share knowledge and expertise on software and supply chain risks, effective practices and mitigation strategies, tools and technologies, and technology gaps. *DOD, GSA, NIST*
- **Static Analysis Tool Exposition:** Recurring event convening tool makers to understand the strength of different tools, identify research needs, and raise public awareness. *OSD, NIST*

4. Additional NITRD Interagency Coordination Activities

The NITRD NCO provides staff support to the information-sharing and strategy-setting activities of three interagency coordination groups in new and emerging challenge areas for Federal IT R&D. These groups do not at this time report budgets under the NITRD PCAs:

- Faster Administration of Science and Technology Education and Research Community of Practice
- Health Information Technology Research and Development Interagency Working Group
- Video and Image Analytics Interagency Working Group

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

***Participating Agencies*: Air Force, DHS, FDIC, IARPA, NARA, NIH, NIST, NOAA, Treasury, VA**

The FASTER Community of Practice engages Federal agency chief information officers and advanced technology specialists to improve interagency communication and coordination and to accelerate deployment of promising technologies from research into operations. The primary focus of FASTER is on addressing multi-agency IT challenges specific to supporting the Federal scientific research enterprise by sharing information on IT protocols, standards, best practices, assessments, and testbeds. FASTER meetings are open to the public; these are advertised in advance on the NITRD website and in the Federal Register.

Health Information Technology Research and Development (HITRD) IWG

***Participating Agencies*: AHRQ, CDC, DoD, FDA, HUD, HRSA, NIDILRR, NIH, NIST, NSF, ONC, VA**

The HITRD Interagency Working Group provides a forum for sharing information about Federal health IT R&D programs, coordinating health IT R&D plans and activities, and promoting synergies across Federal health IT investments. HITRD agencies work collaboratively to articulate health IT R&D needs to policy- and decision-makers and to pursue interagency opportunities that advance IT research, data sharing, integration and connectivity, and innovative health IT systems.

HITRD's focus is on R&D efforts that will lead to more efficient and effective healthcare and improve the quality of American lives through technologies that support effective health monitoring, individualized screening, diagnosis and treatment, disease prevention, disaster and emergency response, and widespread access to health and healthcare information and resources. HITRD activities also contribute to developing a future-focused workforce through R&D investments that help build and sustain a vibrant community of professional health IT researchers and practitioners.

HITRD has developed a strategic health IT R&D framework to identify opportunities and challenges in health IT research. The framework identifies scientific challenges that the group is beginning to address in a series of workshops and publications. This IWG is also collaborating on an assessment of medical device data interoperability (MDDI) with the goal of identifying key knowledge gaps and questions that must be addressed to advance MDDI and thereby improve patient outcomes and safety through data sharing and utilization.

Video and Image Analytics (VIA) IWG

***Participating Agencies*: Air Force, Army, CIA, DARPA, DHS, DoDIIS, DOT, FBI, GSA, IARPA, JIDO, NASA, Navy, NCSC, NCTC, NGA, NIH, NIJ, NIST, NOAA, NSA, NSF, USDA, VA**

The VIA Interagency Working Group is developing a joint strategy for Federal R&D in visible-world video and image analysis technologies with the following goals: advance fundamental and applied research; reinvigorate the Federal VIA R&D portfolio; develop resource-sharing mechanisms; pursue public engagement and outreach; promote technology transfer; develop workforce and research resources; and promote standards and best practices that support emerging Federal needs.

The need for VIA technologies spans a broad spectrum of national priorities and agency missions. The strategic goals mentioned above will have a multiplicative effect on technologies to improve national security and the quality of life for all Americans. VIA technologies are used to enhance public safety, homeland security and national defense, and for justice and forensics applications, among other functions. VIA applications and real-time forensic tools can help protect U.S. cities, borders, troops, and Federal facilities in-country and abroad; monitor fisheries and wildlife to better manage those populations; identify crops and invasive plant species to improve agricultural practices; support efficiency and safety in urban and transportation infrastructures; and facilitate the development of automation-assisted vehicles.

Appendix A. List of Abbreviations

AFOSR	Air Force Office of Scientific Research (DoD)
AFRL	Air Force Research Laboratory (DoD)
AHRQ	Agency for Healthcare Research and Quality (HHS)
AI	artificial intelligence
AI/ML	AI and machine learning
ARI	Army Research Institute (DoD)
ARL	Army Research Laboratory (DoD)
ARO	Army Research Office (DoD)
ARS	Agricultural Research Service (USDA)
BLS	U.S. Bureau of Labor Statistics (DOL)
BRAIN	Brain Research through Advancing Innovative Neurotechnologies Project
CDC	Centers for Disease Control and Prevention (HHS)
CERDEC	Communications-Electronics Research, Development, and Engineering Center (DoD)
CHuman	Computing-Enabled Human Interaction, Communication and Augmentation (NITRD PCA)
CIA	Central Intelligence Agency
CNPS	Computing-enabled Networked Physical Systems (NITRD PCA)
CPS	Cyber-Physical Systems (and a NITRD IWG)
CS	computer science
CSIA	Cybersecurity and Information Assurance (NITRD IWG)
CSP	Cyber Security and Privacy (NITRD PCA)
DARPA	Defense Advanced Research Projects Agency (DoD)
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS S&T	DHS Science and Technology Directorate
DHS/NPPD	DHS National Protection and Programs Directorate
DISA	Defense Information Systems Agency (DoD)
DOC	Department of Commerce
DoD	Department of Defense
DoDIIS	DoD Intelligence Information Systems
DOE	Department of Energy
DOE/CESER	DOE Office of Cyber-security, Energy Security, and Emergency Response
DOE/EERE	DOE Office of Energy Efficiency and Renewable Energy
DOE/EM	DOE Office of Environmental Management
DOE/NNSA	DOE National Nuclear Security Administration
DOE/OE	DOE Office of Electricity Delivery and Energy Reliability
DOE/SC	DOE Office of Science
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
DREN	Defense Research and Engineering Network (DoD)
DTRA	Defense Threat Reduction Agency (DoD)
ECP	Exascale Computing Project (DOE)
ED	Department of Education
EdW	Education and Workforce (NITRD PCA)
EHCS	Enabling R&D for High-Capability Computing Systems (NITRD PCA)
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration (DOT)
FASTER	Faster Administration of Science and Technology Education and Research Community of Practice (NITRD interagency group)
FBI	Federal Bureau of Investigation (DOJ)
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FDIC	Federal Deposit Insurance Corporation
FHWA	Federal Highway Administration (DOT)
FTC	Federal Trade Commission
FY	fiscal year
Gbps	Gigabits per second
GSA	General Services Administration
HCIA	High-Capability Computing Infrastructure and Applications (NITRD PCA)
HCS	high-capability computing systems
HCSS	High Confidence Software and Systems (NITRD IWG)
HDR	Harnessing the Data Revolution Big Idea (NSF)
HEC	High End Computing (NITRD IWG)
HHS	Department of Health and Human Services
HITRD	Health Information Technology Research and Development (NITRD IWG)
HPC	high-performance computing
HPC Act	High-Performance Computing Act, enacted in 1991 and amended by Public Law 114-329
HPCMP	High-Performance Computing Modernization Program (DoD/Army)

Appendix A. List of Abbreviations

HRSA	Health Resources and Services Administration (HHS)
HUD	Department of Housing and Urban Development
IARPA	Intelligence Advanced Research Projects Activity (ODNI)
Interior	Department of the Interior
IoT	Internet of Things
IRAS	Intelligent Robotics and Autonomous Systems (NITRD PCA and IWG)
IT	information technology
ITA	International Trade Administration (DOC)
ITS JPO	Intelligent Transportation Systems Joint Program Office (DOT)
IWG	Interagency Working Group
JIDO	Joint Improvised-Threat Defeat Organization (DoD/DTRA)
LSDMA	Large Scale Data Management and Analysis (NITRD PCA)
LSN	Large Scale Networking (NITRD PCA and IWG)
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NCO	National Coordination Office (NITRD Program)
NCSC	National Counterintelligence and Security Center (ODNI)
NCTC	National Counterterrorism Center (ODNI)
NGA	National Geospatial-Intelligence Agency (DoD)
NICE	National Initiative for Cybersecurity Education
NIDILRR	National Institute on Disability, Independent Living, and Rehabilitation Research (HHS)
NIFA	National Institute of Food and Agriculture (USDA)
NIH	National Institutes of Health (HHS)
NIJ	National Institute of Justice (DOJ)
NIOSH	National Institute for Occupational Safety and Health (HHS/CDC)
NIST	National Institute of Standards and Technology (DOC)
NITRD	Networking and Information Technology Research and Development (Program, or Subcommittee of the NSTC Committee on Science and Technology Enterprise)
NOAA	National Oceanic and Atmospheric Administration (DOC)
NSRDEC	U.S. Army Natick Soldier Research, Development and Engineering Center (DoD)
NRC	Nuclear Regulatory Commission
NRI	National Robotics Initiative
NRL	Naval Research Laboratory (DoD)
NRO	National Reconnaissance Office (DoD)
NSA	National Security Agency (DoD)
NSF	National Science Foundation
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration (DOC)
ODNI	Office of the Director of National Intelligence
ONC	Office of the National Coordinator for Health Information Technology (HHS)
ONR	Office of Naval Research (DoD)
OPM	U.S. Office of Personnel Management
OSD	Office of the Secretary of Defense (DoD)
OSHA	Occupational Safety and Health Administration (DOL)
OSTP	White House Office of Science and Technology Policy
OUSD(R&E)	Office of the Under Secretary of Defense, Research & Engineering (DoD)
PCA	Program Component Area
PI	principal investigator
R&D	research and development
REU	Research Experiences for Undergraduates (NSF)
S&AS	Smart and Autonomous Systems (NSF)
SC	Social Computing (NITRD IWG)
SCC	Smart Cities and Communities (and a NITRD task force)
SDN	software-defined network
SDP	software-defined perimeter
SDX	software-defined Internet exchange
SOCOM	U.S. Special Operations Command (DoD)
SPSQ	Software Productivity, Sustainability, and Quality (NITRD PCA and IWG)
STEM	science, technology, engineering, and mathematics
TIC	trusted Internet connection
Treasury	Department of the Treasury
USAF	U.S. Air Force (DoD)
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
USGS	U.S. Geological Survey (Interior)
USMC	U.S. Marine Corps (DoD)
USPS	U.S. Postal Service
VA	Department of Veterans Affairs
WSRD	Wireless Spectrum Research and Development (NITRD IWG)

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE

SUBCOMMITTEE ON NETWORKING &
INFORMATION TECHNOLOGY RESEARCH & DEVELOPMENT

www.nitrd.gov