Implementation of Federal Prize Authority: Fiscal Year 2014 Progress Report

A Report from the
Office of Science and Technology Policy

In Response to the Requirements of the
America COMPETES Reauthorization Act of 2010

April 2015

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) advises the President on the effects of science and technology on domestic and international affairs. The Office 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. OSTP leads an interagency effort to develop and implement sound science and technology policies and budgets. The Office works with the private sector to ensure Federal investments in science and technology contribute to economic prosperity, environmental quality, and national security. For more information, visit http://www.ostp.gov.

Copyright Information

Department, Agency, Office, and Division Abbreviations

AFRL	Air Force Research Laboratory (part of AF/DOD)
ASA	Office of the HHS Assistant Secretary for Administration (part of HHS)
ASPR	Office of the Assistant Secretary for Preparedness and Response (part of HHS)
CDC	Centers for Disease Control and Prevention (part of HHS)
CMS	Centers for Medicare & Medicaid Services (part of HHS)
CPSC	Consumer Product Safety Commission
CSR	NIH Center for Scientific Review (part of HHS)
DARPA	Defense Advanced Research Projects Agency (part of DOD)
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DTRA	Defense Threats Reduction Agency (part of DOD)
EDA	Economic Development Administration (part of DOC)

Table of Contents

Executive Summary **4**
Introduction **9**
Section 1. Benefits of Prize Competitions and Challenges in the Public Sector 11
Section 2. Support For Scaling the Use of Prize Competitions and Challenges 17
Section 3. Highlights and Trends From Prize Competitions and Challenges Conducted in FY 2014 25
Section 4. Highlights From Prizes Conducted Under the Authority Provided by COMPETES in FY 2014 36
Section 5. Summary of Prizes Conducted Under COMPETES in FY 2014 42
Conclusion 51
Appendix 1: Agency Programs Conducted Under the COMPETES Authority **53**
Appendix 2: Agency Programs Conducted Under Authorities Other Than the COMPETES Authority **196**

Secretary for Administration, DARPA, and NIC. Six agencies have reported on COMPETES challenges for at least three of the four years the authority has been available, and a further seven have reported on challenges under COMPETES or other authorities for at least three years, illustrating that there is healthy, continuous use of prize competitions and challenges by many agencies. The total number of agencies that have conducted prize competitions and challenges to date exceeds 72, according to Challenge.gov.

The total amount of prize money available in FY 2014 COMPETES challenges is five percent greater than the amount offered in FY 2013 – put another way, the average prize purse for a COMPETES challenge in FY 2014 has risen more than 30 percent compared to FY 2013.[53]

Highlights from the 34 prize competitions conducted through the authority offered by COMPETES in FY 2014 include:

DARPA Cyber Grand Challenge (CGC): In FY 2014, DARPA conducted its first prize competition under the authority provided by COMPETES. This prize competition has a very ambitious goal: to engender a new generation of autonomous cyber defense capabilities that combine the speed and scale of automation with reasoning abilities exceeding those of human experts. The CGC is the first-ever tournament for fully automatic network defense systems. CGC cash prizes will total up to $9.75 million. Following the CGC Qualifying Event (CQE) on June 3, 2015, up to eight finalists will each receive $750,000. Following the CGC Final Event (CFE) on August 4, 2016, prizes will be awarded to the first place ($2 million), second place ($1 million), and third place ($750,000) winners.

Currently, without automation, top computer security experts test their skill head-to-head in competitive "Capture the Flag" contests. These contests provide a competition rating for the ability of human experts to locate and comprehend security weaknesses. The CGC will utilize a series of competition events to test the abilities of a new generation of fully automated cyber defense systems. DARPA envisions CGC teams creating automated systems (vice human experts) that would compete against each other to evaluate software, test for vulnerabilities, and generate and apply security patches to protected computers on a network. To succeed, competitors must translate the theoretical results in program analysis research into software applications that automatically detect and fix

[53] This analysis does not include the prize purse for the DARPA Cyber Grand Challenge which, at $9,750,000, represented a significant outlier.

flaws in programs. During a final competition event, automated cyber reasoning systems will compete against each other in real time.

The competition has drawn 104 teams to register comprised of top experts from across a wide range of computer security disciplines including reverse engineering, formal methods, program analysis, and applied computer security competition. Utilizing the authority provided by COMPETES is making it possible for DARPA to work with academic institutions and affiliated teams, large commercial interests not involved in defense contracting, small businesses, small teams of experts, and individuals, most of whom had not worked with DoD before.

HUD's Rebuild by Design Challenge: The authority provided through COMPETES has offered many unique benefits to agencies seeking to stimulate innovation through prizes and challenges. For example, the partnership and gift authorities offered through COMPETES enabled HUD to partner with two philanthropic foundations—the Rockefeller Foundation and the Community Foundation of New Jersey—to conduct Rebuild by Design, a multi-stage regional design competition to promote resilience in the region affected by Hurricane Sandy. Partnerships with non-profit organizations allowed philanthropic resources to be used for 100 percent of the prize awards as well as competition administration. Approximately $5 million was committed collectively on behalf of the six funding organizations (which includes approximately $2 million for the cash prize awards, $2.65 million for competition administration, and $350,000 for the project evaluation). The challenge attracted submissions from 148 teams from more than 15 countries and resulted in seven projects that are being implemented to increase resilience in Sandy-impacted communities in three states. HUD incentivized the implementation of winning designs by committing $930 million made available through the Community Development Block Grant Disaster Recovery (CDBG–DR) program to leverage other public and private funds.

DOT Data Innovation Challenge: In FY 2014, DOT offered their first prize competition under the authority provided by COMPETES. The purpose of the DOT Data Innovation Challenge was to find and highlight data-driven innovations – including web-based tools, data visualizations, mobile apps, or other innovative uses of technology – that address systemic transportation challenges. The incentives for this challenge were entirely non-monetary, including: innovation features on DOT's *FastLane* Blog, a letter of recognition from the Secretary of Transportation, and the winning teams being honored at a

Appendix 1: Agency Programs Conducted Under the America COMPETES Reauthorization Act of 2010

This Appendix provides a complete summary of all prizes competitions conducted in FY 2014 under the prize authority provided to agencies in COMPETES and does not include any of the multiple prize competitions conducted under other authorities in FY 2014 or prior.

List of Challenges

A. Consumer Product Safety Commission

   I. Carbon Monoxide Poster Contest Challenge

   II. Consumer Product Safety App Challenge

B. Department of Defense

   I. DARPA Cyber Grand Challenge

C. Department of Energy

   I. American Energy Data Challenge

   II. National Clean Energy Business Plan Competition – 2014

   III. The SunShot Catalyst Program

   IV. SunShot Prize

D. Department of Health and Human Services

   I. ASA VizRisk

   II. ASPR Ideation Challenge: System for Locating People Using Electricity Dependent Medical Equipment During Public Health Emergencies

   III. CDC Million Hearts Hypertension Control Challenge - 2013

   IV. CDC Million Hearts Hypertension Control Challenge – 2014

   V. CDC Game On! HIV/STD Prevention Mobile Application Video Game Challenge

   VI. CDC "No Petri Dish" Challenge

   VII. CDC Predict the Influenza Season Challenge

B. Department of Defense

I. DARPA Cyber Grand Challenge[66]

Summary: The DARPA Cyber Grand Challenge is the first-ever tournament for fully automatic network defense systems. Currently, top computer security experts test their skill head-to-head in competitive "Capture the Flag" contests. These contests provide a competition rating for the ability of human experts to locate and comprehend security weaknesses. The CGC will utilize a series of competition events to test the abilities of a new generation of fully automated cyber defense systems. DARPA envisions CGC teams creating automated systems (vice human experts) that would compete against each other to evaluate software, test for vulnerabilities, and generate and apply security patches to protected computers on a network. To succeed, competitors must translate the theoretical results in program analysis research into software applications that automatically detect and fix flaws in programs. During a final competition event, automated cyber reasoning systems will compete against each other in real time. The CGC seeks to engender a new generation of autonomous cyber defense capabilities that combine the speed and scale of automation with reasoning abilities exceeding those of human experts.

Solution Type: Software and Apps;

Primary Goals: Solve a specific problem; Build capacity; Engage new people and communities

Results: No prize competitions have taken place in the Cyber Grand Challenge to date. However, 104 teams have registered – including academic institutions, small businesses, and individuals, most of whom had not worked with DoD before, and have produced promising prototype systems.

Problem Statement: The Department of Defense (DoD) maintains information systems using a software technology base comprised of commercial off-the-shelf (COTS) operating systems and applications. This COTS technology base is common to DoD, industry, and the Defense Industrial Base, and the continual discovery of potential vulnerabilities in this software base has led to a constant cycle of intrusion, compromise discovery, patch formulation, patch deployment, and recovery. This defensive cycle is performed by highly trained software analysts; it is the role of these analysts to reason about the function of software and identify and remove novel threats. Manual analysis of code and threats is an artisan process, often requiring skilled analysts to spend weeks or months analyzing a

[66] Challenge Website: www.darpa.mil/cybergrandchallenge; www.cybergrandchallenge.com

problem. The size of the technology base contributes to the difficulty of manually discovering vulnerabilities.

At present, automated program analysis capabilities are able to assist the work of human software analysts. These automation technologies include dynamic analysis, static analysis, symbolic execution, constraint solving, data flow tracking, fuzz testing, and a multitude of related technologies. In the DARPA CGC, a competitor will improve and combine these semi-automated technologies into an unmanned cyber reasoning system that can autonomously reason about novel program flaws, prove the existence of flaws in networked applications, and formulate effective defenses. The performance of these automated systems will be evaluated through head-to-head tournament-style competition.

Entrants will field unmanned systems that will compete head-to-head in an isolated test environment. The results will determine the systems' ability to reason about and mitigate novel software flaws. Awards will be made to the best performing systems in a qualifying event and a final tournament. These two events will be held approximately 12 months apart.

DARPA provided two parallel paths for participating in the CGC: the Proposal Track and the Open Track Proposal Track teams were selected competitively on the basis of proposals submitted in response to a broad agency announcement (DARPA-BAA-14-05). Open Track teams were selected based on applications deemed qualified to compete per Title 15 U.S. C. § 3 719 and CGC rules.

This two-phase process included registration and the submission of an extended application per the CGC rules (see challenge website).

Proposed Goals: The goal of the DARPA CGC is to engender a new generation of autonomous cyber defense capabilities that combine the speed and scale of automation with reasoning abilities exceeding those of human experts. CGC will give DoD the ability to measure the real-world efficacy of unmanned cyber capabilities using a competition rating currently accepted as a measure of excellence for human analysts.

Why a Prize: The CGC will draw widespread attention to the technology issues associated with autonomous software comprehension and motivate entrants to overcome technical challenges to realize truly effective autonomous cyber defense. The competition will challenge the most capable and innovative companies, institutions, and entrepreneurs to produce breakthroughs in capability and performance. Utilizing prize authority under America COMPETES made it possible to work with academic institutions and affiliated teams, large commercial interests not involved in defense contracting, small businesses, small teams of experts and individuals, most of who had not worked with DoD before. In

addition, simple calculations will show that on a full time equivalent basis, the CGC will have instigated large research and development efforts at relatively low cost.

Participants: The CGC will encourage the most capable and innovative companies, institutions, and entrepreneurs to produce breakthroughs in capability and performance. The competition has drawn teams of top experts from across a wide range of computer security disciplines including reverse engineering, formal methods, program analysis and applied computer security competition. Eligibility requirements can be found in the CGC Rules Section 2.1 (see the challenge website). One hundred four entrant teams registered on the challenge website.

Timeline: The CGC was launched October 29, 2013. The two-phase registration process included initial applications due November 2, 2014, and extended applications due February 26, 2015.

Scored Event #1	December 1, 2014
Scored Event #2	April 16, 2015
Qualification Event	June 3, 2015
Trials Begin	March 14, 2016
Trials End	April 3, 2016
Final Event	August 4, 2016

Solicitation & Outreach: The DARPA CGC was announced through several methods including publication in Federal Register, web features, websites, national media, social media outlets, and conference presentations.

Incentives: To date, no cash prizes have been awarded; as a result, amounts have not yet been distributed to appropriation accounts. Because DARPA is the sole sponsor of the CGC, no private funds have been contributed to the program (nor will private funds be contributed as the program/competition progresses to its final conclusion). CGC cash prizes will total up to $9.75 million; non-monetary prizes are not offered. Following the CGC Qualifying Event (CQE) on June 3, 2015, up to eight finalists will each receive $750,000. Following the CGC Final Event (CFE) on August 4, 2016, prizes will be awarded to the first place ($2 million), second place ($1 million), and third place ($750,000) winners.

Evaluation and Judging: No prize authority-enabled events have yet occurred; thus, evaluation and judging have not yet occurred. Due to the potentially subjective nature of judging and evaluation, the CGC is scored and ranked via software automation. Several "dry run" practice events have been conducted to prepare for the qualifying event on June 3, 2015; the results of these dry runs have been beneficial for competitors and organizers.

Partnerships: DARPA is funding various entities within DoD (Space and Naval Warfare Systems Command, Air Force Research Laboratory, Naval Postgraduate School) as well as Federally funded research and development centers (MIT Lincoln Lab) for contracting and specialized technical support in conducting the CGC competition. To raise awareness of the state of the art of automated cybersecurity competition, DARPA entered into a Cooperative Research and Development Agreement with the DEF CON Hacking Conference.

Resources: The DARPA CGC is being organized by Government staff members and support contractors managing logistics, security, infrastructure, administration, information technology services, planning, execution, production, visualization, and software development. The CGC is not being executed by a single entity; rather a cross-disciplinary team of experts from across the United States was assembled to build the software base of the Challenge and develop its automated scoring mechanisms and software platform.[67] Visualization experts from the computer gaming industry were contracted to build novel visualization capabilities for CGC.

Funds were drawn from the Program Element (PE) and projects as follows:

PE	Project	Title	FY14
0602303E	IT-05	Cyber Grand Challenge (CGC)	$10.438M

Results: No prizes have been awarded in the Cyber Grand Challenge to date. The CQE will take place on June 3, 2015, and the CFE is scheduled for August 4, 2016. An initial assessment of the competition to date indicates that prototype systems are being built capable of finding software flaws and patching them on timescales available only to machines. In the DARPA CGC Scored Event #1, competitor systems found and fixed software flaws never before seen by humans.

[67] The Cyber Grand Challenge software platform is available as open source software: https://github.com/CyberGrandChallenge/

Appendix 2: Agency Programs Conducted Under Authorities Other than the America COMPETES Reauthorization Act of 2010

This Appendix provides a summary of select prizes and challenges conducted in FY 2014 under agency prize authorities other than COMPETES. Agency reporting on prizes conducted under non-COMPETES prize authorities was optional, so the list of challenges here may be incomplete.

List of Challenges

A. Department of Commerce

I. Strong Cities, Strong Communities Challenge

B. Department of Defense

I. AFRL Ideas for Annual Computational Cognition Challenge

II. AFRL LabHACK

III. AFRL Non GPS Navigation

IV. AFRL Synthetic Biology for Materials

V. CTNSP Disaster Apps Challenge

VI. CTNSP Explosive Remnants of War and Landmine Reporting Apps Challenge

VII. DARPA Forecasting Chikungunya Challenge

VIII. DARPA Spectrum Challenge

IX. USSSOCOM Reducing Digital Optics Latency

VI. CTNSP Explosive Remnants of War and Landmine Reporting Apps Challenge[143]

Summary: Each year, a large number of civilians are killed and injured by unexploded weapons such as artillery shells, land mines, mortars, grenades and bombs. These explosive remnants of war (ERW) regularly disrupt daily civilian life in post-war and conflict zones. The National Defense University's Center for Technology and National Security Policy's (CTNSP) launched the Explosive Remnants of War and Landmine Reporting Apps Challenge. The competition challenged developers to come up with a mechanism to keep "eyes on the street" and transform ordinary citizen's mobile devices into tools that could be used to report ERW and landmines to the appropriate authorities. Participants were asked to create open-source applications, as well as to leverage existing apps. All submissions had to demonstrate how the new or improved application could produce or improve ERW or landmine reporting, and how the solution would be sustained following the completion of the competition.

This challenge was operated on ChallengePost.

Solution Type: Software and apps

Primary Goals: Find and highlight innovative ideas; Inform and educate the public

Results: The CTNSP ERW and Land Mine Reporting Apps Challenge received 50 challenge registrations, and 5 submissions. The winner, receiving $3000, is an easy to use and easy to understand solution that could be incorporated into any smartphone. The second place winner, receiving $1500, has complementary features for phones that are only SMS-capable, and CTNSP intends to advertise both solutions and potentially offer them as a package to interested parties. USAFRICOM staff are potentially interested in converting the wining app into a medical reporting system for Ebola-like contingencies. The third place winner received $500 for an ERW detector.

VII. DARPA Forecasting Chikungunya Challenge144

Summary: Chikungunya viral infection (CHIKV) is a mosquito-borne viral infection of humans. The recent introduction of chikungunya into the Caribbean has caused substantial morbidity in the population and concern about further spread in the region. As of December 19, 2014 the Pan American Health Organization (PAHO) reports over 24,000 confirmed and one million suspected CHIKV cases in the Americas including over 2,000 cases in the United States. The Department of Defense's (DoD) role in global health includes conducting timely, relevant, and comprehensive health surveillance to promote, maintain,

---

[143] Challenge Website: http://erwlandmineapps.challengepost.com/

[144] Challenge Website: https://www.innocentive.com/ar/challenge/9933617

and enhance the health of military and associated populations. Mathematical and statistical models are useful in predicting the course of infectious disease spread, but no models to date have successfully predicted infectious disease events with sufficient accuracy.

This DARPA Challenge seeks methods to forecast outbreaks and the potential spread of CHIKV throughout the Americas. The forecast will include the number of suspected and confirmed cases and time course in currently-affected islands, as well as the outbreak and course of infection in new locations (including Caribbean, Central, South, and North America). This Challenge also seeks to develop forecasting capabilities for infectious diseases, with the intent of applying these capabilities to the mitigation of infectious diseases outbreaks.

Solution Type: Ideas; Analytics, visualizations, and algorithms

Primary Goals: Solve a Specific Problem; Analytics, visualizations, and algorithms

Results: The challenge is not yet complete, and final results will be reported in FY15. 444 solvers have registered, and a total prize purse of $500,000 is offered.

VIII. DARPA Spectrum Challenge

Summary: As the use of wireless technology proliferates, radios often compete with, interfere with, and disrupt the operations of other radios. The DARPA Spectrum Challenge called on participants to demonstrate radio protocols that can best utilize a given communication channel in congested and contested environments, in support of military operations. The techniques employed by the participants are expected to be representative of next-generation adaptive radio protocols that will be seen in future military and commercial communications systems.

Awards will be made to the best performing systems in two tournament scenarios:

- Competitive Scenario - Two teams attempt to simultaneously transmit a data file from one of their radios to the other. This tests their ability to design a radio that can best overcome interference.
- Cooperative Scenario - Three teams are grouped together with the objective that each team transmit a data file across their radio pair while causing minimal disruption to the other two teams. This tests their ability to design a radio that can operate in the presence of other radios while causing minimum disruption.

Teams compete head-to-head in a structured test environment, using identical radio hardware, to determine the most capable algorithms, as measured by how quickly a block of data can be transmitted from one radio to another.