Testimony of

Dr. Walter Copan
Under Secretary of Commerce for Standards and Technology
and
Director
National Institute of Standards and Technology
United States Department of Commerce

Before the

Commerce, Science, and Transportation Committee
United States Senate

One Year Later: The American Innovation and Competitiveness Act

January 30, 2018

INTRODUCTION

Chairman Thune, Ranking Member Nelson, and Members of the Committee, I am Dr. Walter Copan, Under Secretary of Commerce for Standards and Technology and Director of the Department of Commerce's (DOC) National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss the implementation of the *American Innovation and Competitiveness Act* (AICA) (P.L. 114-329).

Before I begin, let me thank the Committee for your work in the passage of the AICA, which provided new tools and authorities that are helping NIST deliver on its mission.

NIST MISSION

NIST is the nation's measurement science institute. As a non-regulatory agency within DOC, NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Founded in 1901 as the National Bureau of Standards, today NIST develops and disseminates measurements and standards that enable comparison, ensure interoperability, and support commerce. NIST's role is unique: our federal workforce of over 3,000 employees, over half of whom are Ph.D. scientists and engineers, work to create the measurement tools that enable innovation.

NIST's cutting-edge work takes place at two main campuses, the headquarters in Gaithersburg, MD and a campus in Boulder, CO, as well as through NIST personnel in Charleston, SC, Kauai, HI, and Palo Alto, CA. NIST researchers also work in partnership with nine collaborative research institutes across the country to align the most advanced metrology with leading scientific research at U.S. universities and help accelerate the pace of innovation.

The NIST mission has three key themes:

- **Measurement Science:** Creating the experimental and theoretical tools – methods, metrics, instruments, and data—that enable innovation.
- **Standards:** Disseminating measurement standards and providing technical expertise to further the development of documentary standards that enable comparison, ensure interoperability, and support commerce.
- **Technology:** Driving innovation through knowledge dissemination and public-private partnerships that bridge the gap between discovery and the marketplace.

Through work in these areas, NIST has an outsized impact on the U.S. economy, quality of life, and national security.

AICA PASSAGE

To support NIST's work in measurement science, standards and technology, the "American Innovation and Competitiveness Act" (AICA) (P.L. 114-329)—the successor to the America COMPETES Act—became law on January 6, 2017 and updated the authorizing legislation for NIST.

The new law authorizes new programs, recommends changes to improve processes, and supports personnel at NIST. Highlights of the bill related to our laboratory programs include:

- Codifying NIST's continued efforts in cybersecurity;
- Requiring the development of a comprehensive strategic plan for laboratory programs;
- Authorizing research leading to the development of standards for voting security;
- Supporting broader interactions with academia, international researchers, and industry; and,
- Directing NIST to expand its focus on enabling commercial and industrial applications.

The AICA implemented new accountability and oversight provisions for the Hollings Manufacturing Extension Partnership Program (MEP). Further, it authorizes the transfer of direct management of NIST law enforcement and site security through an assigned Director of Security for NIST who reports to the Department of Commerce Office of Security (DOC OSY). The bill acknowledges the importance of allowing employees to attend scientific conferences and workshops to share findings and foster collaboration. It also builds upon previous authority to conduct prize competitions and broadens it to include crowdsourcing and collaborative citizen science to advance our mission.

My testimony will provide additional details on the provisions of the legislation and how NIST has worked to implement them.

CYBERSECURITY RESEARCH (Section 104)

Continuing efforts in cyber standards for critical infrastructure.
Section 104 of the bill made a number of changes to the NIST Cybersecurity program. Under Section 104, NIST has continued its work on the Cybersecurity Framework, Next-Generation Internet of Things (IoT), Addressing Botnet Threats, and Securing Unclassified Government Information.

- **Cybersecurity Framework:** The NIST Cybersecurity Framework (Framework) serves as voluntary guidance for industry, based on existing standards, guidelines and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In 2017 NIST published two public drafts, requesting and addressing public comments, for version 1.1 of the Framework. These updates provided new details on managing cyber supply chain risks, clarified key terms, and introduced measurement methods for cybersecurity. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires that all Federal executive branch agencies use the NIST Framework to manage cybersecurity risk. In 2018, NIST will continue to improve the clarity and

applicability of the Framework focusing on its usability and to communicate the Framework in support of its effective implementation.

- **Next-Generation Safeguards for Information Systems and the Internet of Things:** For the emerging area of Internet of Things, NIST's Cybersecurity for IoT program supports the development and application of standards, guidelines and related tools to improve the cybersecurity of connected devices—which is a network of connected objects that are able to collect and exchange data using embedded sensors such as thermostats, cars, lights, appliances—and the environments in which they are deployed. NIST has issued a draft revision of its widely used Special Publication *Security and Privacy Controls for Information Systems and Organizations* representing an ongoing effort to produce a unified information security framework for the federal government. This latest draft addresses ways various organizations can maintain security and privacy in their interconnected systems. Next-generation safeguards include advanced encryption, secure and reliable connectivity, and cybersecurity for smart grid systems and cyber physical systems. In 2018, NIST is working to broaden strategic collaborations and partnerships with IoT industry experts and its federal government partners to facilitate the development and advancement of IoT interoperability standards, security and best practices.

- **NIST initiative seeks industry solutions in support of the Administration's Botnet initiative:** In Executive Order 13800, the Administration required the Departments of Commerce and Homeland Security to promote stakeholder action against botnets and other automated, distributed threats. NIST worked with NTIA and DHS, in consultation with several other agencies and the private sector, to publish a draft report earlier this month on enhancing the resilience of the Internet against botnets. The report contains draft goals and actions that would improve the resilience of the ecosystem. The Department is collecting stakeholder input on the draft report and will incorporate that input into a final report to the President in May. NIST's National Cybersecurity Center of Excellence (NCCoE) will also develop a "practice guide" to help protect Internet of Things devices from botnet threats that leverages industry solutions. The NCCoE is soliciting "products and technical expertise to support and demonstrate security platforms" for securing IoT from botnet threats, as part of the "Mitigating IoT-Based DDoS Building Block" practice guide.

- **Securing Unclassified Government Information:** Another area to highlight in our cybersecurity research work is the publication of *Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations,* which provides federal agencies with recommended requirements for protecting the confidentiality of CUI that resides on nonfederal systems. NIST has released for public comment the special publication *Assessing Security Requirements for Controlled Unclassified Information,* which is a guideline for any organization seeking to comply with the CUI regulation governing the safe handling of information that is important to the U.S. government. CUI is a diverse classification that includes information involving privacy, proprietary business interests and law enforcement investigations. The public comment period closed on January 15, 2018; NIST will now address public comments before publishing an updated version later this year.

Development of quantum computing and cryptography standards.
NIST has made additional advances in the development of quantum computing and cryptography standards.

Quantum information science research at NIST explores ways to employ phenomena exclusive to the quantum world to measure, encode and process information for useful purposes, from powerful data encryption to computers that could solve problems intractable with classical computers. Some specific areas that are being addressed are:

- **Post-Quantum Cryptography Standardization:** NIST has initiated a process to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms. NIST solicited public comment on draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate algorithms.

- **Qubits:** A team of scientists from the NIST and University of Maryland with the Joint Quantum Institute (JQI) have created a quantum simulator using 53 interacting atomic qubits to mimic magnetic quantum matter. Prior to this breakthrough, researchers had only created quantum simulators of 20 qubits or less. The building of qubit simulators is a key step toward building a full-fledged quantum computer.

- **Single Photon Detector:** Individual photons of light now can be detected far more efficiently using a device patented by a team including NIST whose scientists have overcome longstanding limitations with one of the most commonly used type of single-photon detectors. Their invention could allow higher rates of transmission of encrypted electronic information and improved detection of greenhouse gases in the atmosphere.

- **Chained Bell Test:** NIST recently demonstrated a Chained Bell Test experiment to probe a fundamental assumption of quantum mechanics. Albert Einstein had described the quantum phenomenon as "spooky actions at a distance." The NIST method produced statistically significant results, demonstrating the predicted quantum behavior by using an ion trap setup to probe quantum entanglement by manipulation of ion pairs.

- **Photon Measurement:** Future communications networks that are less vulnerable to hacking are closer to reality because of a NIST invention that measures the properties of single-photon sources with high accuracy. The NIST invention measures detailed information in the spectral properties of photons 10,000 times better than current state-of-the-art devices.

Determine information security vulnerability, challenges and deficiencies, and evaluate effectiveness of implementation standards.
Under this authority, critical continuing work for security includes:

- **Behavioral Cybersecurity:** NIST will assemble a team with experts in cybersecurity, computers science, networking, human actors and cognitive psychology, and sociology to

answer questions such as: What technical information does the public need and how can we make this information more understandable? Why don't individuals practice safe computing? What societal factors influence the adoption of safe computing practices?

- **National Vulnerability Database:** The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol. Over 56,000 entries in the vulnerability database were either new or modified during 2017. In 2018, NIST will continue to research and develop new methodologies to increase efficiencies in analyzing and publishing vulnerability data, while simultaneously improving data reliability.

Codifies research for standards on voting security.
The final new authority under this section codifies the work NIST has been doing on cybersecurity of voting systems.

Voting System Cyber Security Public Working Group: The NIST Voting System Cybersecurity Working Group is the Nation's forum for review and further development of guidance for voting system cybersecurity-related issues, including various aspects of security controls and auditing capabilities. The guidance will inform the development of requirements for the Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG).

NIST conducted the research necessary to develop the Draft Voluntary Voting System Guidelines, version 2.0, progressed interoperability by advancing the Common Data Format (CDF) for election systems, and collaborated with interagency partners in providing additional election security guidance.

NIST research considered significant advances in the technology used in U.S. voting systems, as well as the public's input for addressing the needs of all voters to participate in elections. For example, universal design, mobile devices, and assistive technology now provide much greater accessibility to voters with disabilities. Better quality assurance and configuration management methods, new programming languages, greater fault-tolerance and increased capacity in hardware components, as well as new approaches to data exchange, software assurance, and security have emerged in the last decade.

This research in hardware and software, security, human factors and data exchange led to a draft set of VVSG Principles and Guidelines[1] and five data formats that were discussed and revised through bi-weekly teleconferences with the technical Voting Public Working Groups on *Cybersecurity (121 members), Usability and Accessibility (106 members), and Interoperability (158 members).* In addition to the expert review by the 385 members of these working groups, the draft was adopted at the September 2017 Technical Guidelines Development Committee (TGDC) meeting, and is currently under review by the Election Assistance Commission (EAC) Standards Board and Board of Advisors.

[1] http://collaborate.nist.gov/voting/bin/view/Voting/VVSGPrinciplesAndGuidelines

LAB PROGRAM IMPROVEMENTS (Section 107)

NIST leadership has been working towards developing a long-range strategic plan for NIST's laboratory programs with the goal to identify high-level research priorities to best position NIST looking towards a 10-year horizon. This process, which built on years of work developing short-term prioritized operational plans for each Lab and a year of engagement articulating NIST's values, sought to produce a long-range plan that allows NIST leadership to be proactive instead of reactive in shaping NIST's research environment to address the needs of U.S. commerce in an ever-changing landscape of both federal funding and technical opportunities.

In examining what new technical and organizational capabilities NIST will require in a decade, NIST's leadership considered what are likely to be the requirements of NIST's existing priority areas, such as manufacturing and cybersecurity. What systems will emerge that will require expanded cybersecurity and privacy capabilities? What technologies are likely to change the way cryptography works? What novel products will U.S. manufacturers make, and what new technologies must they use to be competitive? What technical breakthroughs will impact NIST's own business models, and how can NIST lead that change? These questions shaped NIST's identification of opportunities for this strategic vision.

To lay the groundwork for the strategic plan, a scan of the technical landscape was completed, and numerous interviews with NIST senior leadership, former NIST directors, as well as former Visiting Committee on Advanced Technology members were conducted. The interviews explored major opportunities, risks, areas for investment/divestment, NIST culture, leadership, indicators of success, and advice for Commerce Secretary Ross. During a 2-day workshop held at the end of May 2017, a five-person thought leader panel provided their perspectives on the future of technology. One theme that was clear is that science increasingly depends on systems thinking and learning, multimodal data, and multimodal measurements. The second key theme was that NIST has a place and a part in teaching people about measurement science and ensuring measurements are being conducted to get the best data out. During these early stages of discussion, three possible areas for growth were identified in vertical capabilities, meaning associated with specific disciplines: bioscience; quantum science; and IoT. In horizontal capabilities, meaning cross-cutting areas, potential areas for growth include data science and artificial intelligence and systems-level thinking and modeling.

NIST's opportunities for impact are inescapably tied to the Institute's mission and historic role. NIST's future must build on a solid foundation of technical expertise and stakeholder engagement. Since its founding in 1901, NIST has been known as "Industry's National Laboratory," dedicated to supporting U.S. competitiveness. To continue to be the bedrock of innovation in the U.S., NIST must grow new capabilities over the next decade. With investments in emerging key areas coupled with continued dedication to areas of traditional expertise and contribution, NIST will ensure impact in the coming decades.

NIST's current priorities—including manufacturing, technology transfer, cybersecurity, quantum technologies, and disaster resilience—will continue to align with national imperatives for the decades to come. The manufacturing sector will continue to be a driving force of innovation and

productivity for the U.S. economy. Transitioning technologies effectively from laboratory to market is the seed corn for our innovation economy as well as entrepreneurship. The need for strong and practical cybersecurity approaches are growing rapidly as digital systems integrate into more of our lives and commerce. The very real hazards of natural disasters must be addressed through effective standards and technologies, and America's built infrastructure and communities must be able to withstand and recover from those events. Quantum-based devices, communications and cryptography hold great promise for the U.S. and for the future of measurements and standards, and our Nation must be positioned to address market, technology and cyber threats from others in this domain. While the NIST strategic priorities will not change, they will be influenced by new and rapidly evolving technologies.

To extend its reach and amplify its influence, NIST will work with stakeholders within the Institute, across government, in industry and academia on the opportunities with greatest impact potential for the Nation. These interdisciplinary areas—or themes—are at the forefront of science and technology, and will therefore require the collective talent and ingenuity of researchers and leaders across the NIST laboratories.

Theme 1: Provide a foundation of trust in new industries

- Enabling the future **bioeconomy**. As proof-of-concept laboratory work in engineering biology meets the market realities of bringing lab science into commercial introduction, there are questions about how to compare biological products, measure whether desired outcomes are realized, and optimize biological systems for desired behaviors. NIST will deliver tools and standards to measure biological technologies, outputs, and processes that will enhance economic sectors from healthcare to manufacturing and beyond.

- Unleashing the economic potential of **IoT**. Robust, secure, and competitive technology advances in the Internet of Things must be built on a solid foundation of measurement and standards. NIST will develop new tools and approaches for IoT systems security, establish technologies to relieve network congestion and device interference, and facilitate greater confidence in device interoperability.

Theme 2: Apply new technologies to revolutionize mission delivery

- Enhancing mission-critical research through **Artificial Intelligence (AI)** and data. NIST will develop resources and expertise to apply AI, machine learning, and big data techniques to measurement science, including curated datasets to train and test AI systems, model AI behavior and compare AI systems, as well as to apply AI to research efforts where big data requires the application of advanced learning algorithms.

- Revolutionizing commerce through quantum measurements. In May, 2019, the International System of Units (SI) is slated to be redefined with units based on fundamental constants of nature, and NIST must lead in this transition to quantum definitions. NIST will use its world-leading quantum science expertise to develop physical reference standards and "self-calibrating" sensors that will enable a world where measurement devices are ubiquitous, reliable, and affordable.

NIST CAMPUS SECURITY (Section 113)

The legislation supports the Department's efforts to continue to improve overall security. Security and safety begins with the leadership of NIST, and I am ultimately responsible for the organization's security and safety culture and performance. The Department also continues to take steps to improve the physical security at NIST. NIST, working with the Department, is committed to improving the security culture at both NIST campuses. Let me highlight the steps we have taken to ensure successful implementation of the legislation's provisions.

The AICA authorized in the Department of Commerce Office of Security (OSY) supervisory authority for law enforcement and site security at NIST. OSY manages and implements all security, emergency management, and threat investigations across the Department and its thirteen bureaus and operating units.

Responsibility for security clearly does not rest solely with OSY. Security is also directly related to safety at NIST. At NIST, I am responsible for ensuring the security of the personnel, facilities, property, information and assets in accordance with applicable laws, regulations, Executive Orders, and directives. The Director of Security is responsible for advising and assisting heads of operating units. Thus, OSY and NIST mutually support one another to protect the personnel, mission, information, and infrastructure at NIST's facilities.

I am committed to a comprehensive assessment of the roles and responsibilities of OSY and NIST at NIST's two campuses, in Gaithersburg, MD, and Boulder, CO, as recommended in the GAO report. Currently, OSY is charged with delivering integrated law enforcement and security services and protection, while NIST is responsible for ensuring the physical security of the buildings. In practice, this means that NIST has primary responsibility for providing and maintaining electronic locks, surveillance devices, and alarms at NIST's campuses. NIST also is responsible for establishing local campus security procedures, and the maintenance and management of the physical security systems such as access control systems, intrusion detection systems, identification badging, and other security and safety systems designed to protect NIST assets.

In turn, OSY provides the security personnel to monitor security cameras, undertake routine patrols of NIST's campuses and buildings, and provide emergency assistance. It also oversees a contract guard force that secures entry points to the campuses.

SCIENTIFIC AND TECHNICAL COLLABORATIONS (Section 202)

NIST hosts over 110 conferences a year with over 13,000 attendees on our campus. The AICA enables streamlining of conferences at NIST and is critical for not only conferences but for the promotion of measurement science and technology transfer that is key to the NIST mission.

In August of 2017, NIST participated in a Department of Commerce pilot effort to review, change and streamline the conference pre-approval process. One significant policy change that resulted

from this pilot effort was to now permit NIST to approve personnel to attend conferences at which the costs to attend did not exceed $200,000, which greatly facilitated the approval process.

NIST continues to evaluate conference attendance policies to ensure that our scientists and engineers are able to provide their expertise for the benefit of the U.S.; conference participation is critical for scientific openness and effective technology transfer.

NIST EDUCATION AND OUTREACH (Section 306)

To further support NIST's efforts in promoting science and technology, NIST has already begun using the authority conferred under the AICA to support the mission of NIST and broaden the public's awareness and understanding of measurement science.

Promoting Public Awareness of Measurement Science: NIST is producing a series of special reports on the worldwide consensus plan to redefine four of the seven basic units of measurement in the SI and we are funding a documentary film to help explain the case for redefinition.

Hiring Authority: The new hiring authority in AICA gives NIST the opportunity to broaden its hiring processes. NIST is working with OPM to obtain critical pay authority for NIST Fellows and has submitted a formal request to institute this process. This request was submitted in November of 2016 and is pending approval.

STEM UNDERGRADUATE EXPERIENCES (Section 309)

NIST has a long history of supporting the STEM (Science, Technology, Engineering, and Mathematics) career paths and growing the next generation of young scientists. The NIST Summer Undergraduate Research Fellowship (SURF) Program is designed to inspire undergraduate students from across the country to pursue careers in STEM through a unique research experience that supports the NIST mission. SURF students from across the country have the opportunity to gain valuable, hands-on experience, working with cutting edge technology in one of the world's leading research organizations and home to three Nobel Prize winners. Over the course of 11 weeks, SURF students at NIST contribute to the ongoing research of one of the seven NIST labs in Gaithersburg and Boulder. SURF provides opportunities for undergraduates to engage in hands-on research pertaining to the NIST mission under the guidance of a NIST scientist or engineer. To date 2,600 undergraduates have participated in the program from U.S. institutions of higher education including Puerto Rico and last summer NIST hosted 213 students.

PRIZE COMPETITION, CROWDSOURCING AUTHORITY (Sections 401 and 402)

To tackle ambitious problems in support of the NIST mission, NIST has long used challenges to bring a community together. In the early 1970's, for example, NIST issued a public challenge to develop a data encryption standard to support computer security.

NIST continues to use challenges to incentivize action around important technical issues. For example, NIST's Global City Teams Challenge (GCTC) provides a collaborative platform for local governments, non-profits, academic institutions, and corporations to form project teams in areas such as smart and secure cities and communities.

The Federal government, and NIST's, use of prizes has ramped up significantly in recent years, in part due to explicit legal authorities, expanded under the AICA, to conduct cash and non-cash prize competitions. In addition to providing the explicit authority to offer cash prizes to winners, this authority allows Federal agencies to partner with private sector, for-profit and nonprofit entities. Since 2015, NIST has launched eleven prize competitions, all of which are posted on challenge.gov. The topics of these competitions range from the development of advanced materials that better absorb impacts such as those experienced by athletes and the warfighter, to the development of software applications using NIST scientific data, to new virtual reality environments for heads-up displays that can be worn by first responders. The last of these is part of a larger open innovation program housed in NIST's Public Safety Communications Research division (PSCR) of the Communications Technology Laboratory in Boulder, CO. PSCR is focusing on key areas for technology acceleration through prize competitions including location based services and enhanced user interfaces for the increased effectiveness of deployed technologies.

As we continue to build our experience in prize competitions, we are finding new opportunities to use this mechanism to further our mission. The NIST Program Coordination Office is a focal point for Institute-wide activity in prize competitions: they serve as the White House point of contact for NIST's prize activities, convene a Community of Interest in Prizes and Challenges that allows staff to share lessons learned and best practices and host an internal website with resources for any staff interested in learning more about using prize competitions.

NIST benefits greatly from the resources provided by the General Services Administration under the AICA. NIST posts all its prize opportunities on the GSA website challenge.gov, and has used the GSA's free platform to host several of our prize competitions. Challenge.gov provides additional valuable content and background about this topic at https://www.challenge.gov/toolkit/, which includes some content provided by NIST to be shared among the community.

Crowdsourcing and Citizen Science: The authority in this Act for agencies to conduct crowdsourcing and citizen science activities is also of interest to NIST. NIST has a history of citizen science activities that includes decades-long high-frequency radio wave propagation reports for NIST radio station WWV, which broadcasts time and frequency information 24 hours per day, 7 days per week to millions of listeners worldwide from Boulder, Colorado. We are exploring the potential to further amplify the Institute's programmatic goals using the AICA authority.

MEP PROGRAM UPDATES (Section 501)

Hollings Manufacturing Extension Partnership (MEP)

With Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers, MEP has instituted the programmatic modifications authorized in the bill.

Cost-Share: The Act changed the non-federal/federal cost sharing ratio for MEP Centers from a 2:1 minimum matching ratio to a 1:1 ratio. As a result, MEP Centers have increased partnering opportunities with manufacturers.

Re-competition: Another important change contained in the AICA required Centers to undergo a re-competition after ten years of consecutive funding. Prior to the AICA, some Centers had not been competed since their initial funding. The re-competitions for all Centers that were not competed in the past 10 years were by April of 2017. Surveys for Center project impacts go out one year after project completion, so the full network of Centers will have initial survey results of the impact of the re-competition in Spring 2019.

Evaluations: The AICA provided clear guidance on Center evaluations. Under the legislation, a Center is to undergo a peer evaluation during its third and eighth-year of operation with a Secretarial review at year five, which used by NIST in determining whether a Center's performance merits continued NIST funding. MEP has instituted new processes by which these evaluations, known as Panel Reviews and Secretarial Reviews, are conducted. MEP is now piloting the new process for Centers which have entered their third year of operations.

Advisory Board: The MEP Advisory Board provides guidance and assesses the overall performance of the Program. Under AICA, the membership of the Board was updated to require no fewer than 10 members with at least one community college representative, allowing MEP to increase the size of the Board and broaden its geographical reach and membership expertise. Following the passage of the AICA, MEP added ten new members to expand the Board and to replace members whose terms had expired. The AICA also instituted several changes to the Center Oversight Boards regarding membership, composition, term limits and conflicts of interest policies. These have been incorporated in the General Terms and Conditions of each Center's cooperative agreement.

Competitive Awards: The legislation also clarified the criteria to make special competitive awards. These awards allow Centers in good standing to receive additional funds based on the availability of funding for projects outside the scope of their base award.

CONCLUSION

NIST is proud of the positive impact it has had and of the improvements we have been able to make with the AICA authorization. NIST maintains its longstanding commitment to advancing measurement science in order further innovation and increase the competitiveness of U.S. industry. NIST's broad technical portfolio positions the agency to contribute productively and rapidly to emerging national needs. With NIST's dedicated technical staff, one-of-a-kind facilities, and objective, non-regulatory role we are well positioned to have an outsized impact on the U.S. economy, quality of life, and national security. With the continued support of this Committee, NIST will continue to thrive in its important mission to promote U.S. innovation and industrial competitiveness.

Thank you for the opportunity to testify on NIST's implementation of AICA. I would be happy to answer any questions that you may have.

Walter G. Copan, PhD.
Under Secretary of Commerce for Standards and Technology and NIST Director

Dr. Walter G. Copan was confirmed by Congress as Under Secretary of Commerce for Standards and Technology and NIST Director on October 5, 2017.

As NIST Director, Dr. Copan provides high-level oversight and direction for NIST.

He has had a distinguished and diverse career as a science and technology executive in large and small corporations, U.S. government, nonprofit and other public-sector settings.

Dr. Copan formerly served as president and CEO of the IP Engineering Group Corporation, providing services in intellectual property strategy, technology commercialization and innovation. Until June 2017, he was founding CEO and chairman of Impact Engineered Wood Corporation, an advanced materials technology company. He also is a founding board member of Rocky Mountain Innovation Partners, where he led technology transfer programs and innovation services on behalf of the U.S. Air Force Academy, U.S. federal labs and academic institutions and helped foster entrepreneurial businesses in the Rocky Mountain West. He also served with the National Advisory Council to the Federal Laboratory Consortium for more than 5 years, providing industry inputs to advance the U.S. economic impacts of the federal laboratory system.

From 2010–2013, Dr. Copan served as managing director of Technology Commercialization and Partnerships at DOE's Brookhaven National Laboratory (BNL). Among his accomplishments were leading the creation and implementation of the new DOE technology transfer mechanism, "Agreement for Commercializing Technology" (ACT), to facilitate collaborations between the federal labs and U.S. corporations. He led the "Startup America" initiative on behalf of DOE for entrepreneurial business creation, and he initiated the DOE's new Small Business Innovation Research – Technology Transfer (SBIR-TT) program, which built upon the experiences of NIST. He served as founding partner and board member of the "Accelerate Long Island" alliance for innovation, economic development and early stage investment.

From 2005–2010, Dr. Copan was executive vice president and chief technology officer at Clean Diesel Technologies, Inc., an international technology development and licensing firm. He spearheaded the company's transformation, growth and listing on NASDAQ (CDTI), as well as the company's subsequent merger. Prior to joining CDTI, Dr. Copan served at the DOE's National Renewable Energy Laboratory (NREL) as Principal Licensing Executive, Technology Transfer. There, he led organizational changes that strengthened relationships with industry and the investment community, and led to the more productive commercialization of energy-related technologies.

After earning dual B.S./B.A. degrees in chemistry and music from Case Western Reserve University in 1975, Dr. Copan began his career in chemicals and materials research at the Lubrizol Corporation (now part of the Berkshire Hathaway Group). He earned a Ph.D. in physical chemistry from Case Western in 1982, and subsequently held leadership positions at Lubrizol in research and development, strategy, business unit management, venture capital, and mergers, acquisitions and strategic alliances in the U.S. and abroad. As managing director, Technology Transfer and Licensing, from 1999–2003, he was responsible for Lubrizol's corporate venturing and open innovation, technology strategy, business development, intellectual assets and the technology licensing business.

Dr. Copan is a patent holder, has authored numerous professional publications and presentations, and has served on the boards of many organizations, including the Licensing Executives Society (LES) USA and Canada, where he recently served as regional vice president for LES USA. He has contributed to the U.S. National Academy of Sciences, the Council on Competitiveness, the World Intellectual Property Organization and the United Nations on innovation, technology transfer, energy and economic development matters.