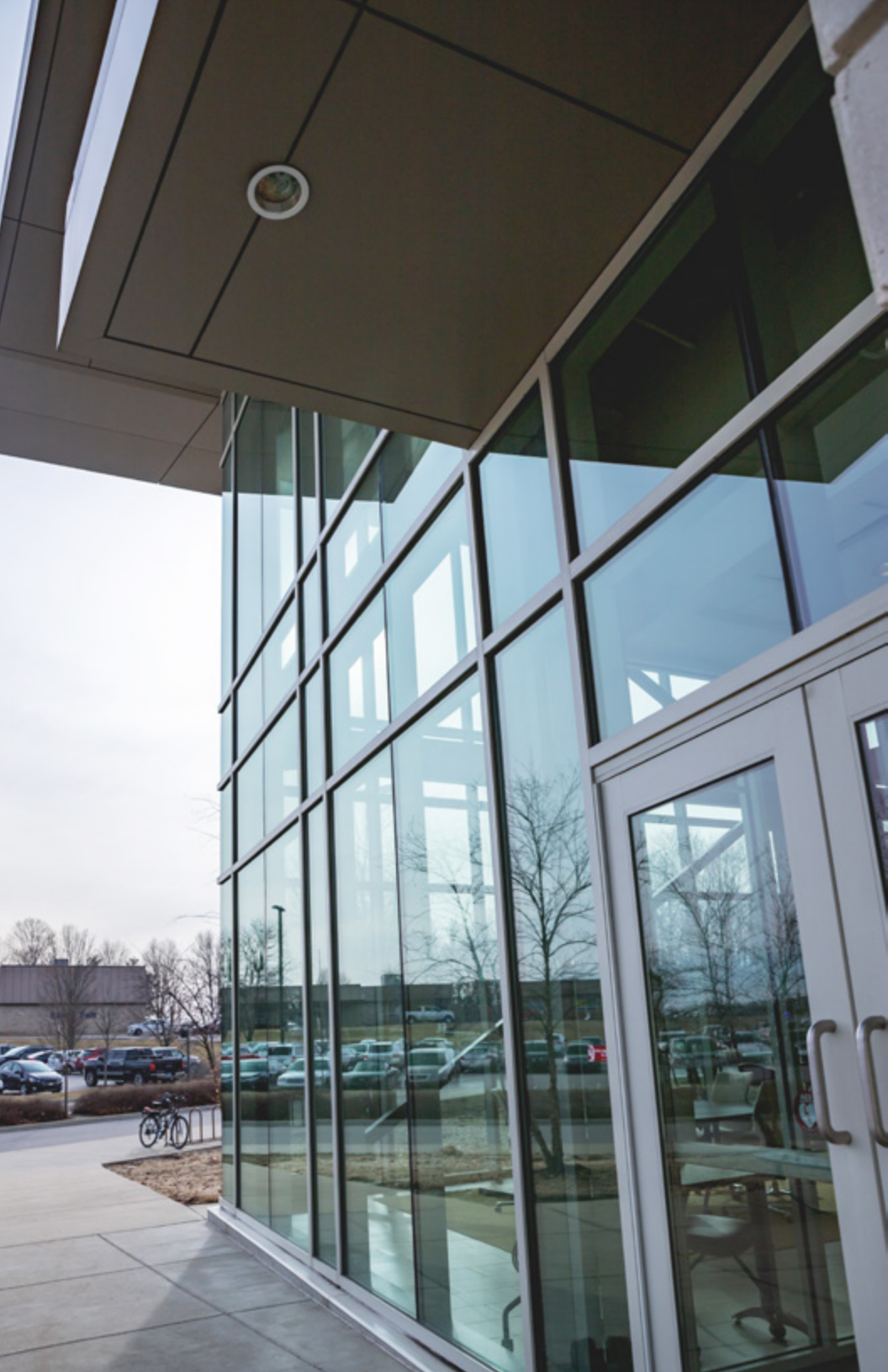
# CENTER FOR APPLIED CYBERSECURITY RESEARCH

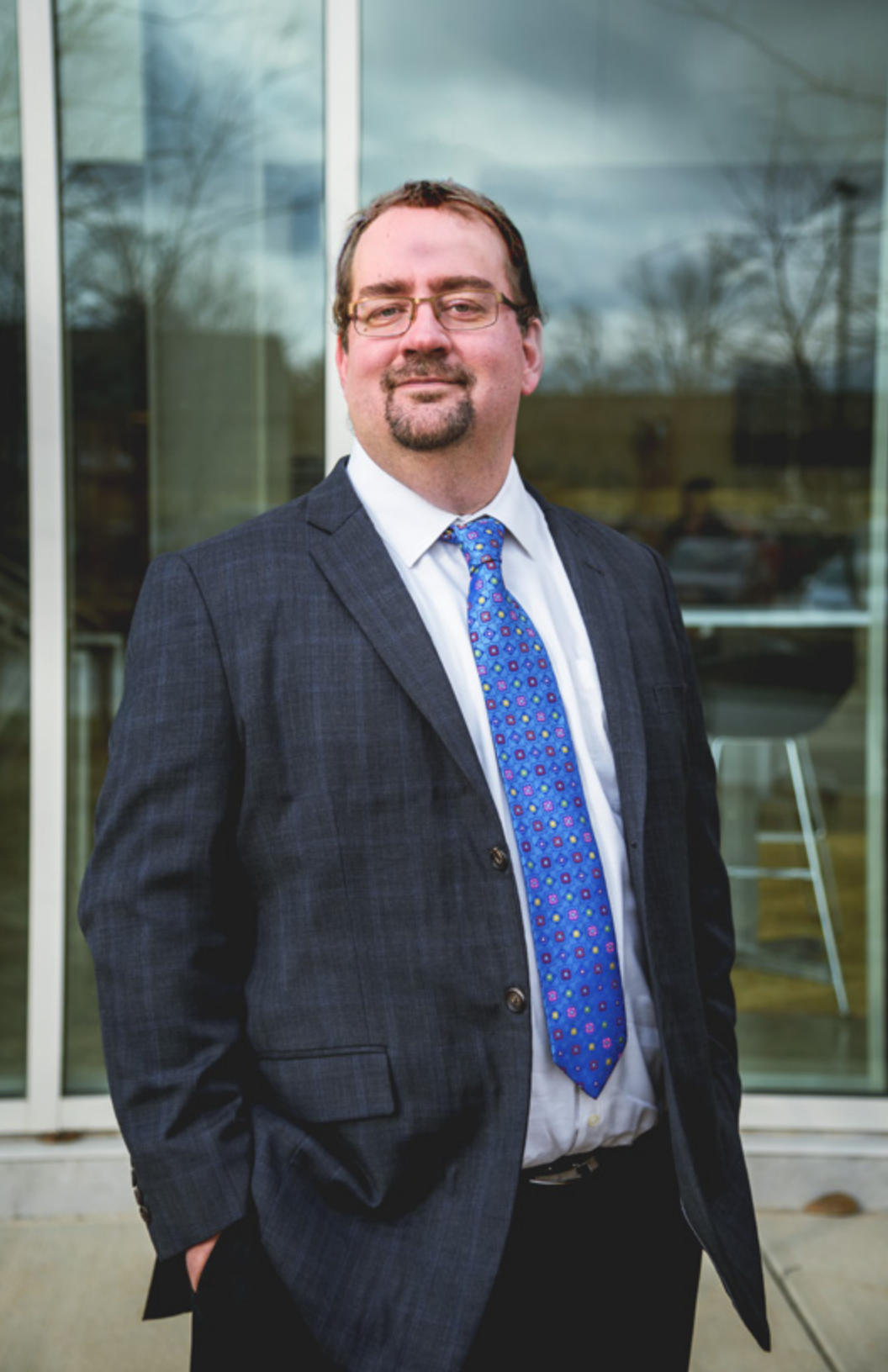
PERVASIVE TECHNOLOGY INSTITUTE

# Leadership in ACTION

## July 2017 – Dec. 2018 Annual Report



# Table of CONTENTS



## Dear friends of the Center for Applied Cybersecurity Research,

Cybersecurity continued to maintain front-page prominence in the media this year, from data breaches that have become unfortunately common to playing a critical role in emerging technologies such as artificial intelligence and automated vehicles.

It is against this backdrop that we present CACR's 2017-2018 Annual Report. In our report, you will read not simply a story of an increasing number of grants received, projects initiated, positive impacts on the state, and amount of research furthered, but also a story of growing leadership in addressing the cybersecurity challenges that face our nation, our state, and our institutions of higher learning and their invaluable scientific research.

CACR is leading in tackling the growing list of the most difficult challenges in cybersecurity in some of the most challenging environments, of building bridges between educational institutions and the government, of leading the conversation about cybersecurity, of bringing needed resources to the Hoosier state, of training the next generation, and of enabling research.

Key to CACR's success has been collaboration with and support from our many partners and supporters, to include the **National Science Foundation**, **Naval Surface Warfare Center Crane Division**, the **Department of Homeland Security**, multiple partner universities, and of course Indiana University's researchers and operational cybersecurity staff.

Moreover, CACR's success is a direct result of the Center's staff, most of whom wear multiple hats in leading and working across our diverse portfolio, and provide both operational acumen and applied research. This team's ability to stretch what is possible on a routine basis is truly admirable. Our Fellows have also been invaluable in their support, and we are sincerely grateful.

It is with a sense of pride in this year's accomplishments, and acknowledging that the future holds both greater promise and greater challenges, that I present the attached report.

**Von Welch**
Director, CACR

# About CACR

CACR is Indiana University's flagship center for cybersecurity, serving as an integrator for research across the university's different schools and organizations. CACR is distinctive in addressing cybersecurity from a comprehensive, multidisciplinary perspective. CACR draws on IU's wide range of scholarly expertise in computer science, informatics, accounting and information systems, criminal justice, law, organizational behavior, and public policy, as well as the extensive practical cybersecurity experience of its operational units. CACR is the only university-level center in the country that involves legal, policy, economic, and behavioral research, along with technical expertise.

Founded in 2003, CACR is a research center affiliated with the Pervasive Technology Institute at Indiana University.

CACR is a member of the Indiana University cybersecurity community, which includes the **OmniSOC** and **ResearchSOC cybersecurity operations centers**, the **National Science Foundation Cybersecurity Center of Excellence (Trusted CI)**, the **Maurer School of Law**, the **Kelley School of Business**, **REN-ISAC**, the **University Information Policy Office**, the **University Information Security Office**, and the **School of Informatics, Computing, and Engineering**.

# CACR's MISSION

CACR's mission is to provide people with the knowledge and skills they need to manage cybersecurity risks in complex, challenging environments where standard cybersecurity practices do not suffice. It does so through a combination of thought leadership, applied research, training and education, operational services, and extensive interdisciplinary collaboration.

# Shaping the CONVERSATION

CACR is changing the way the profession thinks about cybersecurity. In September of 2017, O'Reilly Media published **Security from First Principles**, a foundational work of thought leadership designed to enable the information security community to assess any security guide, policy, or standard—and even create new ones. Authored by CACR's Craig Jackson, Scott Russell, and Susan Sons, Security from First Principles outlines seven key information security practice principles and provides an accessible path through the jargon-heavy environment of cybersecurity.

## 7 Cybersecurity First Principles

COMPREHENSIVITY

OPPORTUNITY

RIGOR

MINIMIZATION

COMPARTMENTALIZATION

FAULT TOLERANCE

PROPORTIONALITY

# Cybersecurity leadership for the NATION

**During the year, CACR expanded its leadership role by addressing some of the most difficult cybersecurity challenges facing the nation, addressing national defense and national scientific research projects.**


## ResearchSOC: Cybersecurity for the nation's science

Launched in October 2018, the Research Security Operations Center is unique in the world: it is the only organization with the mission to provide operational cybersecurity services to NSF-funded facilities and projects, while at the same time seeking to further research in cybersecurity. Funded by a $5 million award from the NSF, ResearchSOC helps make scientific computing resilient to cyberattacks and capable of supporting trustworthy, productive research. CACR leads this collaborative effort that brings together existing cybersecurity services and expertise from Indiana University, including the OmniSOC and REN-ISAC; Duke University; the Pittsburgh Supercomputing Center; and the University of California San Diego. Initial clients include three NSF Large Facilities.

## Trusted CI enters sixth year and expands activities

trustedci.org

CACR's ongoing leadership in protecting the cybersecurity of over $7 billion in NSF-funded research was confirmed with a $2.5 million grant extension for the NSF CCoE (Trusted CI) for expansion of its activities. CACR is the lead organization for the NSF CCoE, in collaboration with the National Center for Supercomputing Applications, the Pittsburgh Supercomputing Center, and the University of Wisconsin-Madison. Now in its sixth year of service, Trusted CI has been at the forefront of the NSF community in building a set of technical, policy, and cultural best practices necessary to ensure the security of that infrastructure and ensure the trustworthy nature of the science it produces. As the lead organization for Trusted CI, CACR hosts the annual NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. Drawing over 100 members of the NSF community from around the country, the NSF summits promoted a platform where communities with interest in supporting NSF science projects collaborated to address core cybersecurity challenges. In 2018, CACR Director Von Welch presented the keynote speech "Five Years Backwards and Forward" at the 2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure. The NSF invited Welch to present this talk as part of the NSF OAC webinar series.

## CACR and NSWC Crane team up for national impact through PACT

As part of its ongoing relationship with **Naval Surface Warfare Center, Crane Division (NSWC Crane)**, CACR received a two-year, $1.9 million award from the U.S. Department of Defense to fund the real-world piloting of the Principles-based Assessment for Cybersecurity Toolkit, or PACT. Developed by CACR program director Craig Jackson and CACR senior policy analyst Scott Russell in collaboration with NSWC Crane, PACT provides cybersecurity professionals with guidance to efficiently develop custom cybersecurity solutions for unusual challenges in the naval environment and operational technologies like control systems.

## Cybersecurity for the world's largest physics experiment

CACR took part in ensuring the safety of data from the Large Hadron Collider (LHC) through a $870,000 grant from the **Institute for Research and Innovation in Software for High-Energy Physics (IRIS-HEP)**. CACR's role in the project is to oversee security of the Open Science Grid, a high-throughput computing platform that allows scientists at any institution, even those without high-end computing resources, to work with massive data sets such as those coming from the LHC. CACR's work will help ensure the availability and integrity of data, which is critical to the productivity and trustworthiness of science.

## Developing best-practice models and a cyber infrastructure blueprint

Building on its expertise leading the NSF Cybersecurity Center of Excellence, CACR is part of a team awarded a $3 million grant to conduct a pilot study for a potential Cyberinfrastructure Center of Excellence. The goal of this pilot program is to develop a model for a full Cyberinfrastructure Center of Excellence that will serve the NSF community in developing and operating the software and hardware systems critical to the nation's research.

## Providing a marketplace for trusted software

As part of a team that includes the Morgridge Institute for Research and the University of Wisconsin, CACR continued to advance software assurance by providing the **Software Assurance Marketplace (SWAMP)**. Funded by the Department of Homeland Security, SWAMP is committed to bringing a transformative change to the software assurance landscape by providing a national marketplace with continuous software assurance capabilities for researchers and developers. By offering multiple software analysis tools and a library of software applications with known vulnerabilities, the SWAMP is committed to making it easier to integrate security into the software development life cycle.

## Ensuring the integrity of scientific data and research

To enable safe and secure data sharing, CACR also continued its leadership — with Von Welch as principal investigator — of the NSF-funded **Scientific Workflow Integrity with Pegasus (SWIP)** project. SWIP improves the security and integrity of scientific data by integrating cryptographic integrity checking and provenance information into the Pegasus workflow management system. It is expected that solutions implemented for this project will be generic enough to apply to other workflow systems and applications, thereby helping a broad range of research with concerns about data integrity. Building on SWIP foundations, CACR partnered with the **Renaissance Computing Institute (RENCI)** on the **Integrity Introspection for Scientific Workflows (IRIS)** project. This project will automatically detect, diagnose, and pinpoint the source of unintentional integrity anomalies in scientific workflows executing on distributed computing infrastructure. Finally, CACR is supporting, through expert guidance on cybersecurity and privacy challenges, RENCI, the University of North Carolina-Chapel Hill, Duke University, and the city of Durham, NC, on a project that aims to allow scientists to share and analyze data across institutional boundaries while keeping that data safe and in compliance with regulations. The three-year project was funded by a $3 million NSF grant.

**$7 Billion**
of NSF science secured

**$8.5 Million**
in new NSF awards

**$1.9 Million**
new DOD award

### A Collaborative Leader

**Trusted CI:** CACR leads a 7-entity collaboration

**ResearchSOC:** CACR leads a 4-entity collaboration

**SWIP:** CACR leads a 3-entity collaboration

**CRADA** with NSWC

**Partners** on numerous DHS and NSF awards

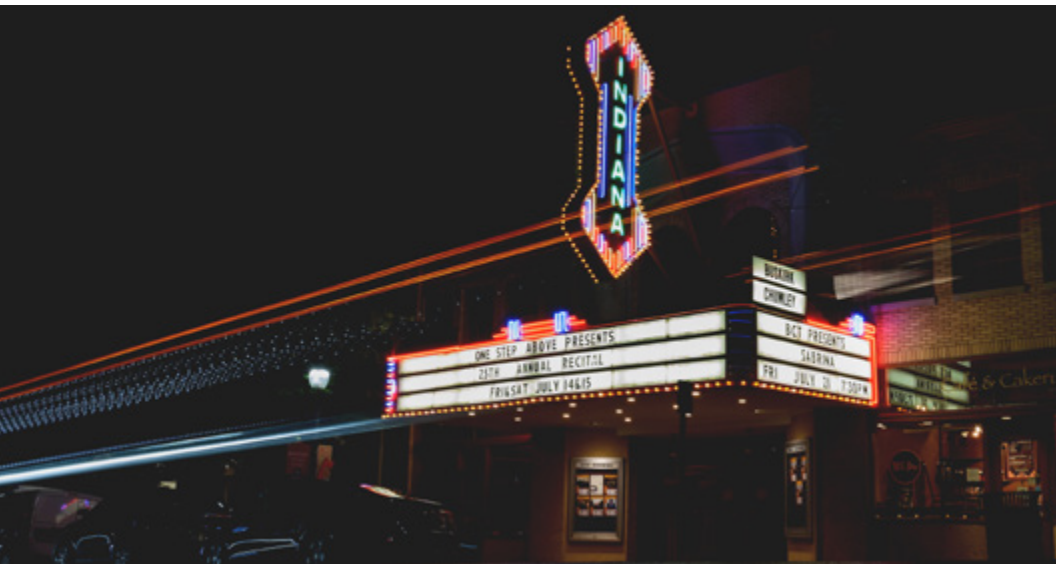
# **Leadership** for a BETTER INDIANA

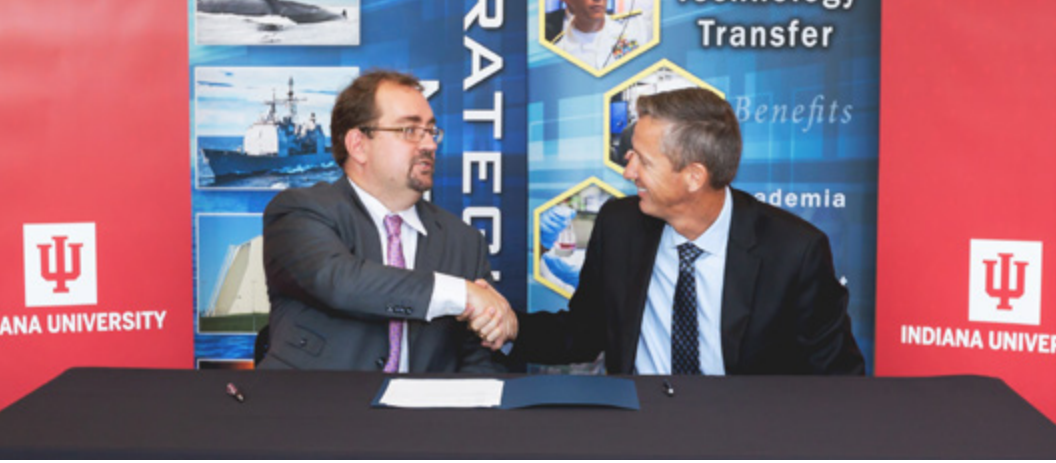
**CACR is a driver for economic growth in South Central Indiana, but CACR contributes more than just the funds that create highly valuable cybersecurity jobs. CACR's initiatives also helped to prepare young Hoosiers for careers in cybersecurity, a key element of STEM education.**

## Bringing resources to the Hoosier state

CACR continues to be a leader in bringing financial resources to South Central Indiana. Through CACR's efforts, this year 15 awards were received or extended totaling over $11 million of new federal funds. Over its lifetime, CACR has brought a total of $31 million award dollars to the South Central Indiana region. While methods of determining local economic impact vary, a commonly accepted estimate of the "ripple effect" is $2.50 of positive economic impact for every grant dollar spent, thus making CACR's lifetime impact on the region over $77 million dollars.

Moreover, the Indiana Business Research Center at Indiana University Kelley School of Business estimates that for every new job directly supported, an additional three jobs are created through ripple effects. With CACR's growth to 20 employees, an estimated 60 new jobs have been created in the Bloomington and South Central Indiana area to date.



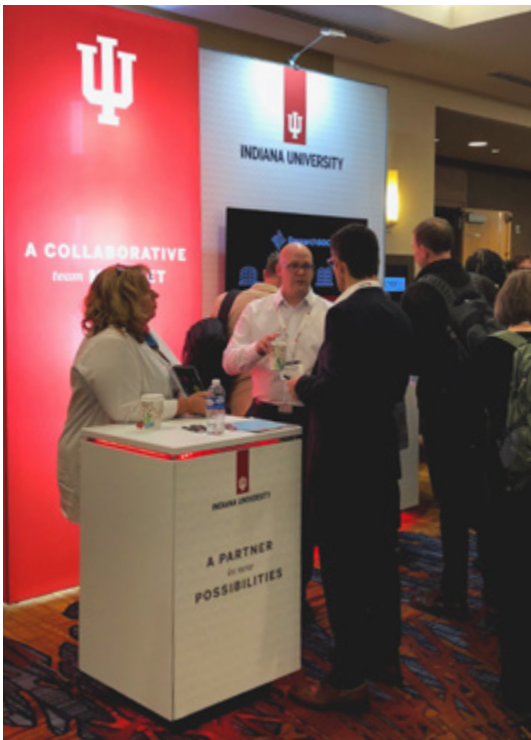



## NSWC Crane and CACR: Building for the next success

The success of CACR and NSWC Crane partnership was further recognized with the re-signing of the cooperative research and development agreement (CRADA), a follow-on collaboration between NSWC Crane and CACR, which was originally executed in 2016. The goal is to strive for state-of-the-art technology advancements and increase collaboration to improve capabilities in the areas of software assurance and trusted artificial intelligence. The agreement strengthens the state's position to attract and retain new projects, jobs, and talent.

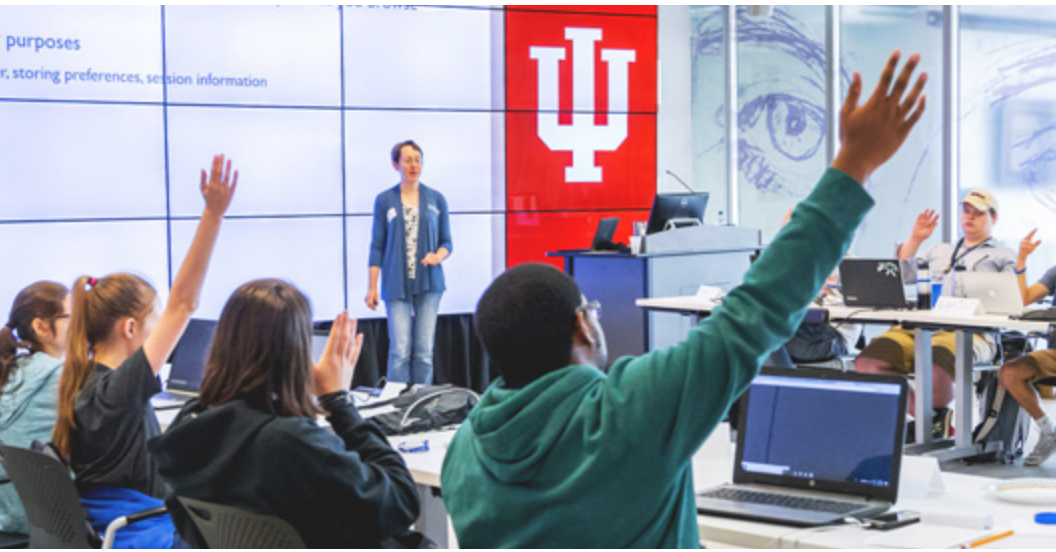
## Connecting Indiana businesses and CACR knowledge

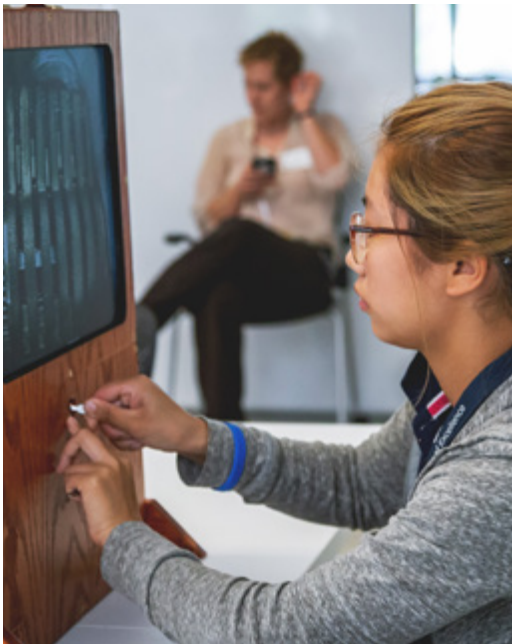
CACR ensured its vast knowledge of cybersecurity was shared here at home. In October 2018, Director Von Welch presented at **Cybertech Midwest**. Cybertech is the cyber industry's foremost B2B networking platform, featuring cutting-edge content by top executives, government officials, and leading decision makers in cybertechnology. The Cybertech Midwest 2018 event featured a conference and exhibition on global cyber threats, solutions, innovations, and technologies.

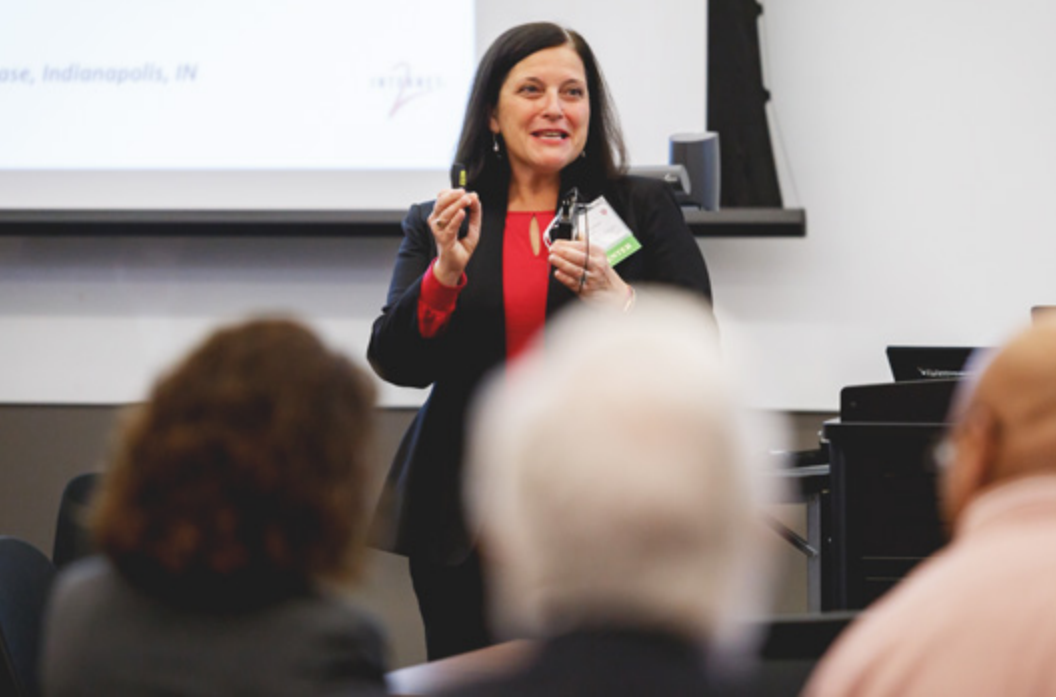


## Educating Indiana's next generation

CACR also helped to ensure that tomorrow's Hoosier IT professionals are cybersecurity-smart. In June 2018, CACR hosted its "**Security Matters Cybercamp**" for high school students. The two-day camp included hands-on sessions in network security, cryptography, data forensics, website penetration testing, and jobs in cybersecurity. CACR also co-hosted a Security Matters Cybercamp for college students with Indiana University's **Center for Women in Technology (CeWiT)**.





## Sharing knowledge across the state

In October 2017, CACR hosted the **Cybersecurity Summit at IU Bloomington**. The CACR event brought together leaders from government, academia, and business for a one-day event and covered a range of issues affecting cybersecurity risk management on both a local and national level. CACR also hosted the first Cybersecurity Research Acceleration Workshop and Showcase in October 2017 at Indiana University-Purdue University Indianapolis. With the goal of building bridges between researchers and practitioners, Trusted CI and Internet2, a technology community founded by U.S. research and education institutions, organized the event.

**$77 million**
in lifetime economic impact

**$27 million**
2017-18 economic impact

**60 new jobs created**

# Leadership for a STRONGER IU

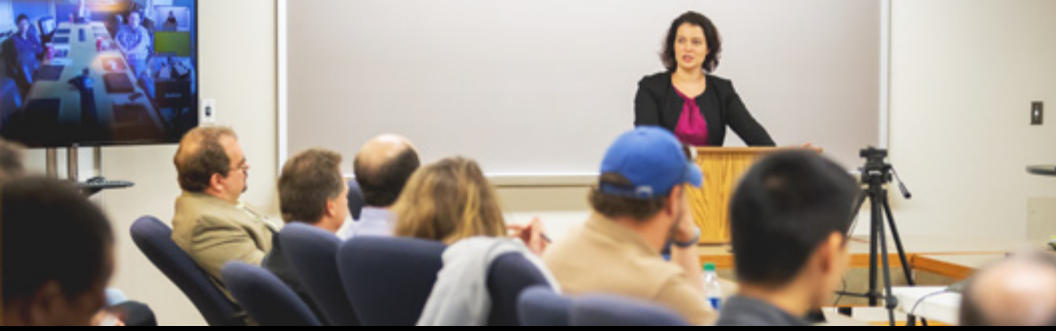
**During the year, CACR provided new opportunities to further the university's research mission while serving as a key force in achieving IU's strategic objectives.**

## Building collaborations across IU

CACR's awards continue to build collaborations across IU. The ResearchSOC award pulls together IU operational cybersecurity expertise with faculty from SICE. The SWIP project draws on SICE cybersecurity expertise. The PACT project draws on the expertise from the School of Education. Three new fellows joined CACR: Associate Professor Damir Cava, Professor Dan Hickey, and Associate Professor Raquel Hill.

## Fulfilling IU's strategic plan

Through the expansion and renewal of key partnerships, CACR continued to meet the challenge presented in IU's Bicentennial Strategic Plan to "facilitate university-industry collaboration by identifying opportunities to work in areas such as cybersecurity with Indiana defense-related institutions like NSWC Crane and the Indiana National Guard."



## Igniting broad collaborations: The CACR Speaker Series

The **CACR Security Speaker Series** brings cybersecurity experts from across the nation to present their current research and real-world experiences to IU faculty, staff, and students. These presentations can yield some exciting collaborations that bring together faculty researchers, students, and even professionals from the private sector

One such CACR-facilitated collaboration followed a CACR Security Speaker Series presentation by Ms. Maria Rerecich, director of electronics testing at Consumer Reports (CR) magazine. During Ms. Rerecich's visit to Indiana University, a plan was fashioned for a project in which students from IU's Cybersecurity Risk Management Capstone course would, in support of Consumer Reports Digital Standard Initiative, analyze CR's Digital Standard with an eye toward updating it in light of recent developments, such as the European Union's General Data Protection Regulation (GDPR), and then applying the revised standard to payment and banking apps, consumer electronics, and cloud services. At the end of the course, the students are traveling to Yonkers to tour CR headquarters and present their findings to the Consumer Reports team.

## Supporting stronger global IU relationships

CACR participated in the **Australian National University (ANU)** visit to IU, in which ANU and IU strengthened their relationship with a new agreement to bolster research collaboration, exchanges, and teaching. ANU operates Australia's fastest supercomputer, highest-performance research cloud, and largest data repository.

**16:1**

2017-18 CACR RETURN ON UITS INVESTMENT

# CACR Leadership Team

CACR Director **Von Welch** has more than a decade of experience developing, deploying, and providing cybersecurity for private and public sector high performance computing and distributed computing systems.

Administrative Director **Leslee Bohland** has more than two decades of experience in management and accounting.

Program Director **Craig Jackson** has research and development interests that include information security program development and governance, cybersecurity assessment design and conduct, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defenses.

Chief Security Analyst **Mark Krenz** is focused on cybersecurity operations, research and education. He has more than two decades of experience in system and network administration. He serves as the CISO of the ResearchSOC and the Software Assurance Marketplace (SWAMP).

Chief Security Analyst **Susan Sons** focuses on secure software engineering, ICS/SCADA security, operational security practice for research and development organizations, and security for legacy technologies in high-stakes applications. Susan serves as Information Security Officer for Open Science Grid and Deputy Director of the Research SOC.

## CACR Staff

CACR staff help manage the daily operations of the center. CACR staff includes administrative, management, and external relations support, as well as security and policy analysts.

**Ishan Abhinit**
Senior Security Analyst

**Emily K. Adams**
Principal Security Analyst

**Diana Borecky**
CACR Events and Communications Manager

**Mary Conley**
Senior Security Analyst

**Randy Heiland**
Senior Systems Analyst/ Programmer

**Ryan Kiser**
Systems Analyst

**Austin Mitts**
IT Support Specialist

**Tori Richardson**
Administrative Assistant

**Scott Russell**
Senior Policy Analyst

**Zalak Shah**
Systems Analyst

**Anurag Shankar**
Senior Security Analyst

**Mike Stanfield**
Senior Security Analyst

## Fellows and Key Liaisons

CACR has more than a dozen Fellows, each one bringing unique insights and connections to the Center, allowing it to capitalize on the interdisciplinary strengths of Indiana University and the broader community. Fellows represent a wide range of perspectives, including law, policy, ethics, and informatics.

**Mark Bruhn**, Indiana University former Associate Vice President for Assurance and Public Safety
**Fred H. Cate**, Maurer School of Law
**L. Jean Camp**, School of Informatics, Computing, and Engineering
**Damir Cavar**, College of Arts and Sciences, Department of Linguistics
**Jake Chen**, School of Informatics and Computing, IUPUI
**Robert Cowles**, Brightlite Information Security
**Rachel Dockery**, Maurer School of Law
**Arjan Durresi**, Department of Computer and Information Science, IUPUI
**David P. Fidler**, Maurer School of Law
**Daniel Hickey**, School of Education
**Raquel Hill**, School of Informatics, Computing, and Engineering
**Apu Kapadia**, School of Informatics, Computing, and Engineering
**Steven Myers**, School of Informatics, Computing, and Engineering
**Scott Orr**, School of Engineering and Technology, IUPUI
**Scott J. Shackelford**, Kelley School of Business
**Robert Templeman**, Naval Surface Warfare Center Crane
**Joseph Tomain**, Maurer School of Law
**XiaoFeng Wang**, School of Informatics, Computing, and Engineering
**Xukai Zou**, Department of Computer Science and Information Scienc, IUPUI

## Other IU Cybersecurity Community Members

**OmniSOC** | www.omnisoc.iu.edu
**Protect IU** | www.protect.iu.edu
**REN-ISAC** | www.ren-isac.net
**Indiana University Cybersecurity Risk Management Program**
www.cybersecurityprograms.indiana.edu
**The SICE Masters of Science in Secure Computing Program**
www.cs.indiana.edu/programs/ms-secure-computing.html

## Acknowledgment

CACR's work is funded by the **IU Office of the Vice President for Information Technology**, the **IU Office of the President**, the **Department of Homeland Security**, and the National Science Foundation (grants 1547272, 1642070, 1659367). None of the opinions expressed in this report should be assumed to represent the opinions of funding entities.

# CENTER FOR APPLIED CYBERSECURITY RESEARCH

PERVASIVE TECHNOLOGY INSTITUTE

2719 E. 10th Street, Suite 231, Bloomington, IN 47408 | cacr@iu.edu | (812) 856-0458