CENTER FOR APPLIED CYBERSECURITY RESEARCH

INDIANA UNIVERSITY
BICENTENNIAL
200 YEARS

2019 CACR ANNUAL REPORT

January 1, 2019–December 31, 2019

TABLE OF CONTENTS

3 From the director

4 About CACR

4 CACR's mission

6 2019 highlights

8 Leading the nation in cybersecurity

14 Leading Indiana to a more secure future

17 Leading IU to help drive discovery

21 CACR leadership team, staff, and fellows

FROM THE DIRECTOR

Dear friends of the Center for Applied Cybersecurity Research,

The increasing cybersecurity threat to research and higher education became even clearer in 2019, as publications such as *Inside Higher Education* and *The Wall Street Journal* reported a ramping up of state-sponsored hacking targeting U.S. top universities. A dozen cloud providers were the victim of compromising attacks, stealing the sensitive research and other data of hundreds of companies. The national headlines hit close to IU's home in Bloomington, Indiana, in November when a local medical records company fell victim to a ransomware attack with a $17K ransom demand. Some industry observers labeled 2019 as the worst year yet.

Yet for CACR, 2019 was a year of achievement and recognition. Through an exceptional $12.5M five-year grant extension for **Trusted CI**, the National Science Foundation (NSF) recognized the value of the CACR-led Cybersecurity Center of Excellence's contributions and leadership in securing more than $7B in national research, both in the past and into the future. The **State of Indiana** engaged CACR to provide election cybersecurity training in advance of the 2020 elections. And, in May, Indiana University leadership named its first executive director for cybersecurity innovation while providing additional resources to CACR to lead initiatives to help secure more than $600M of university research.

CACR's work also continued to catalyze collaborations across IU. Examples abound. The Research Security Operations Center (ResearchSOC) award pulls together IU operational cybersecurity expertise with faculty from the **Luddy School of Informatics, Computing, and Engineering**. The Scientific Workflow Integrity with Pegasus project draws on Luddy's cybersecurity expertise. The Principles-based Assessment for Cybersecurity Toolkit project draws on the expertise from the **School of Education**. CACR's collaboration with the **Maurer School of Law** exposes law students to legal issues in the cybersecurity domain. The new SecureMyResearch project, supported jointly by the **Office of the Vice President for Information Technology** and the **Office of the Vice President for Research**, will catalyze research with cybersecurity and compliance requirements across IU. CACR's Fellows program reaches across five IU schools, IUPUI, and beyond. We are sincerely grateful to our Fellows for their invaluable support.

Collaboration with and support from our many partners and supporters have been foundational to our success. These include the **National Science Foundation**, **Naval Surface Warfare Center Crane Division**, the **Department of Homeland Security**, Indiana University's **Office of the Vice President for Research**, and the **Office of the Vice President for Information Technology**, an extensive list of partner universities, and IU's researchers and operational cybersecurity staff.

Last in mention but first in importance are the members of CACR's staff. These individuals provide leadership and expertise while working across multiple and varied projects. This team routinely raises the bar on the definition of excellence.

With achievement and recognition come increased expectations. I am proud of CACR's accomplishments and confident that our service and leadership will exceed those expectations, and so present our 2019 Annual Report.

Von Welch
Director, CACR
Executive Director for Cybersecurity Innovation

ABOUT CACR

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.

Founded in 2003, 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 operational and technical expertise.

Indiana University has taken a leadership position addressing difficult cybersecurity challenges through its unique operational, research, and academic programs. CACR is a proud member of the university's cybersecurity community, which includes the **OmniSOC** cybersecurity operations center, the **Global Research Network Operations Center (GlobalNOC)**, the **National Science Foundation Cybersecurity Center of Excellence (Trusted CI)**, **ResearchSOC**, the **Maurer School of Law**, the **Kelley School of Business**, **Research and Education Networks Information and Analysis Center (REN-ISAC)**, the **University Information Policy Office**, the **University Information Security Office**, the **Ostrom Workshop**, and the **Luddy School of Informatics, Computing, and Engineering**. It is these programs, and their extensive collaborations, that have made IU an acknowledged "quiet powerhouse" in cybersecurity for higher education and research.

Led by Brad Wheeler, vice president for information technology and CIO, IU operates one of the most advanced cyberinfrastructures of any university in the world. IU is home to **Big Red 200**, a Shasta supercomputer built by Cray, a Hewlett Packard Enterprise company.

Exemplars of CACR work

National

Trusted CI Leadership for the NSF cybersecurity ecosystem

ResearchSOC Cybersecurity services for the nation's greatest research

PACT The Principles-based Assessment for Cybersecurity Toolkit for assessing the toughest cybersecurity problems

SWAMP The Software Assurance Marketplace for continuous software assurance capabilities for researchers and developers

State

Election security Preparation for election officials in all 92 Indiana counties for cybersecurity incidents related to the 2020 general election and beyond

Security Matters cybercamps Day camps for K8+ focusing on all things cybersecurity

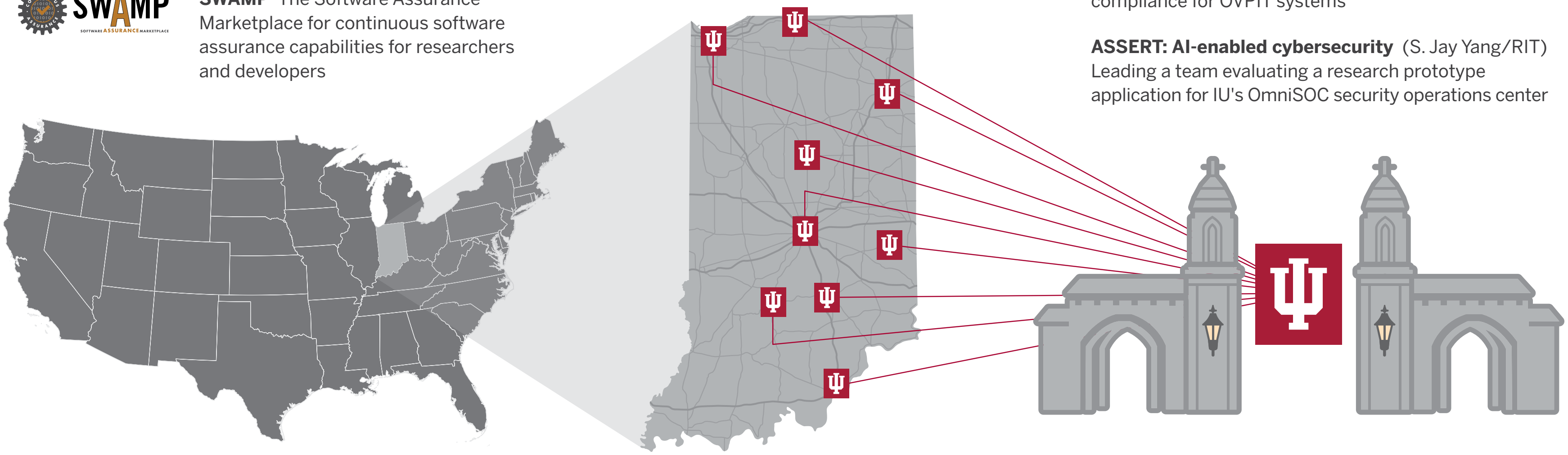
Indiana University

Executive director for cybersecurity innovation (EDCI) Leveraging IU's cybersecurity strengths to address challenges faced across the nation and expanding the role of CACR

SecureMyResearch Reducing the cybersecurity burden on researchers while enhancing research data security at IU

HIPAA compliance Providing oversight of HIPAA compliance for OVPIT systems

ASSERT: AI-enabled cybersecurity (S. Jay Yang/RIT) Leading a team evaluating a research prototype application for IU's OmniSOC security operations center



Big Red 200 is the state of Indiana's fastest supercomputer and one of the fastest university-owned supercomputers in the nation. The GlobalNOC manages 20+ state, national, and international networks, operates **NOAA's N-Wave** network, and is the NOC for **Internet2**, serving 300+ universities, government agencies, and affiliated organizations. IU's **University Information Technology Services** manages over 1,000 technology-enabled classrooms. In 2019, CACR received $400,000 from the Office of the Vice President for Information Technology and returned $419,487.

CACR is a research center affiliated with the **Pervasive Technology Institute (PTI)** at Indiana University. PTI consists of seven centers and two labs and focuses on improving the quality of life in the state of Indiana and the world through novel research, innovation, and service delivery in information technology and informatics.

2019 HIGHLIGHTS

1. Trusted CI received $12.5M/five-year grant renewal, recognizing its value and service and ensuring its long-term continuation.
2. IU appointed Von Welch executive director for cybersecurity innovation, a university-wide role responsible for leveraging IU's cybersecurity operational and research strengths.
3. CACR's team of experts helped prepare election officials in all 92 Indiana counties for cybersecurity incidents related to the 2020 general election and beyond.
4. The Principles-based Assessment for Cybersecurity Toolkit (PACT) team delivered their final assessment report in their engagement with Scripps Institution of Oceanography (SIO) and UC San Diego.

KEY NUMBERS

$13,223,607

CACR 2019 awards

$44,301,971

CACR lifetime awards

$92,000,000

Lifetime regional economic impact

LEADING THE NATION IN CYBERSECURITY

ABOVE: 2019 NSF Cybersecurity Technology Transition to Practice Workshop

CACR's ongoing leadership in protecting the cybersecurity of more than $7B in NSF-funded research was confirmed with a $12.5M grant extension for the NSF Cybersecurity Center of Excellence (Trusted CI) for expansion of its activities. CACR is the lead organization for Trusted CI, in collaboration with the **National Center for Supercomputing Applications**, the **Pittsburgh Supercomputing Center, Internet2, Lawrence Berkeley National Laboratory (Berkeley Lab), and the University of Wisconsin–Madison**.

Trusted CI: leading the NSF cybersecurity ecosystem

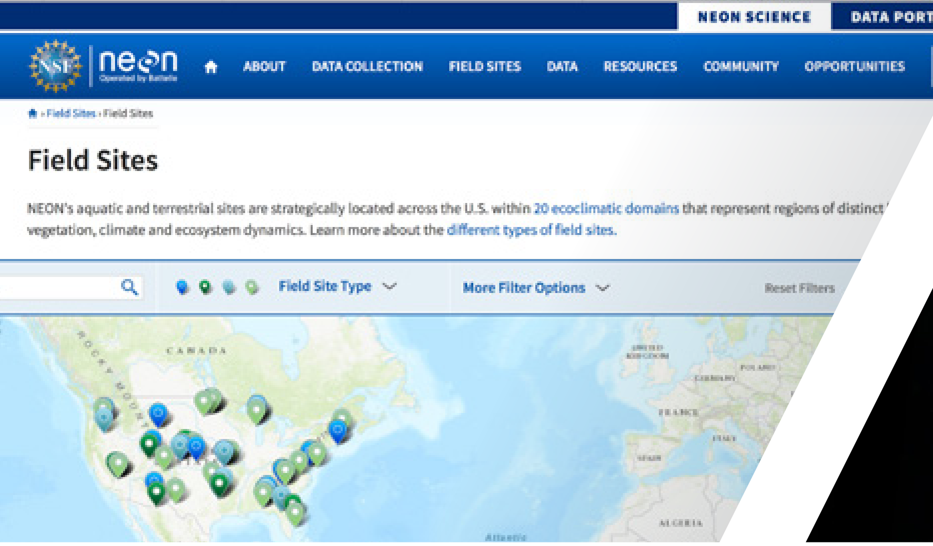
Now in its seventh year of service, Trusted CI has been at the forefront of the NSF community in building a set of technical, policy, and cultural best practices necessary to ensure the security of that infrastructure and ensure the trustworthy nature of the science it produces. Trusted CI positively impacted more than 260 NSF projects since its inception in 2012 and provided more than 300 hours of training to the community in 2019.

Trusted CI collaborates with:

- The **Science Gateways Community Institute (SGCI)** by advising gateway developers on cybersecurity issues and providing security reviews for existing gateways
- The **Engagement and Performance Operations Center (EPOC)** to assist at the intersection of networking performance and cybersecurity
- **ESnet** on developing a threat profile for open science
- **European Union Authentication and Authorisation for Research and Collaboration** project on enabling use of identity federations for international research collaborations
- **Open Science Grid**, **XSEDE**, and **REN-ISAC** on situational awareness for NSF cyberinfrastructure projects
- NSF CICI Regional Cybersecurity Collaboration projects: **CORE**, **SAC-PA**, **SCEPTRE**, and **SouthEast SECURE**
- The **Software Sustainability Institute** by sharing best practices on software engineering and operating a CI center
- The **ResearchSOC** on providing operational services to the research community—sharing leadership and coordinating to provide the NSF community with comprehensive cybersecurity leadership and resources
- The **CI CoE Pilot** project to share experiences on engaging the NSF community and advise on cybersecurity aspects of cyberinfrastructure

2019 NSF Cybersecurity Summit

- The **Cal Poly Pomona Scholarship for Service** project to support workforce development in cybersecurity
- **Internet2** and **InCommon** on federated identity and access management for research collaborations
- The **EDUCAUSE Cybersecurity Program**, led by the **Higher Education Information Security Council (HEISC)**, supporting higher education institutions as they improve information security governance, compliance, data protection, and privacy programs
- **Wise Information Security for collaborating E-infrastructures (WISE)**, sharing a common goal to support research through the development of appropriate cybersecurity practices balanced with the research mission, and collaborating to ensure that cybersecurity frameworks, templates, and policies for international infrastructures for research will grow increasingly aligned and framework implementations more interoperable
- **FABRIC** on cybersecurity transition to practice



Field Sites

NEON's aquatic and terrestrial sites are strategically located across the U.S. within 20 ecoclimatic domains that represent regions of distinct vegetation, climate and ecosystem dynamics. Learn more about the different types of field sites.

NEON's aquatic and terrestrial sites

Rendering of young galaxy from NRAO website

NSF Cybersecurity Summit: promoting collaboration to improve cybersecurity

As the lead organization for Trusted CI, CACR hosted the annual NSF Cybersecurity Summit. Drawing over 140 members of the NSF community from around the country, the NSF summit promoted a platform where communities interested in supporting NSF science projects collaborated to address core cybersecurity challenges. In 2019, Stefan Savage, professor in the systems and networking group at the University of California, San Diego, presented the keynote speech, "Advancing cybersecurity as an evidence-based discipline."

TTP Workshop: putting research into practice

Trusted CI, Indiana University's Innovation and Commercialization office, Microsoft, and the National Science Foundation (grant ACI-1547272) hosted the 2019 Cybersecurity Technology Transition to Practice (TTP) Workshop in Chicago on June 19, 2019. The goal of the TTP program is to enable researcher and practitioner collaboration to accelerate cybersecurity research to practice in industry, academia, government, or open source via matchmaking, business model coaching, and workshops.

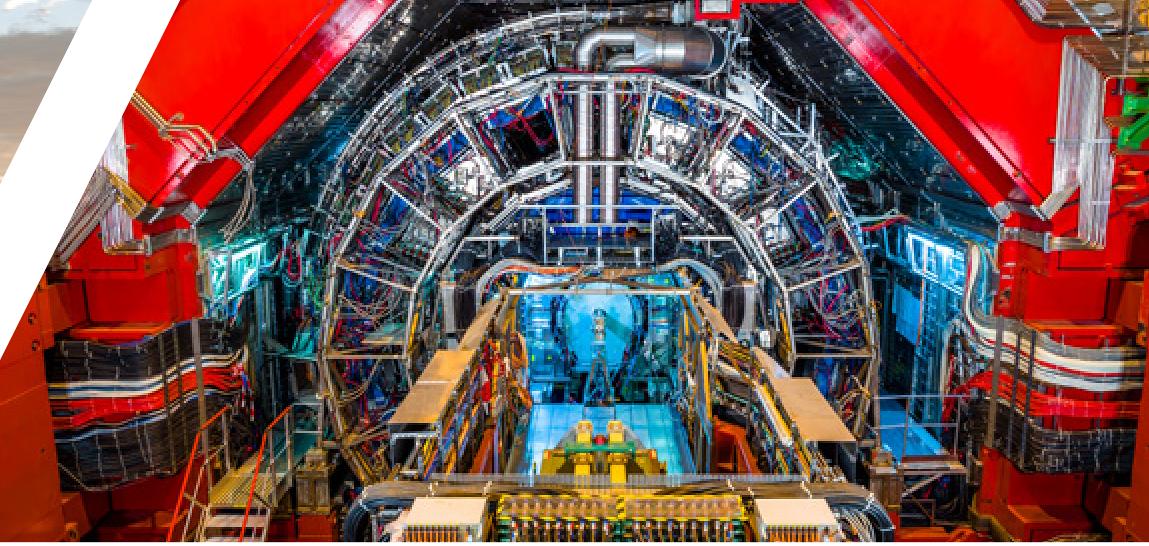
PACT: collaborating for custom solutions

The **Principles-based Assessment for Cybersecurity Toolkit (PACT)** is a tool for assessing the toughest cybersecurity problems. CACR chief policy analysts developed the tool in collaboration with NSWC Crane. As a naval installation, Crane uses technologies that many would consider atypical, and which require custom cybersecurity solutions. The PACT team delivered their final assessment report in their engagement with Scripps Institution of Oceanography (SIO) and University of California, San Diego in collaboration with NSWC Crane.

ResearchSOC: promoting cybersecurity for the nation's greatest research

As 2019 drew to a close, the **Research Security Operations Center (ResearchSOC)** was poised to onboard its first client, the **National Radio Astronomy Observatory (NRAO)**. Launched in October 2018, ResearchSOC 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 $5M 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.

NRAO radio telescopes in San Agustin, New Mexico



ATLAS (A Toroidal LHC ApparatuS) at the Large Hadron Collider (LHC)

SWAMP

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, SWAMP works to make it easier to integrate security into the software development life cycle.

OSG (IRIS-HEP)

The **Open Science Grid (OSG)** facilitates access to distributed high-throughput computing for research in the U.S. and worldwide. The **Institute for Research and Innovation in Software for High Energy Physics (IRIS-HEP)** serves as an active center for software R&D and transforms the operational services required to ensure the success of the **Large Hadron Collider** scientific program. CACR provided cybersecurity leadership services to these projects, with CACR team members serving as the projects' chief information security officers.

CI CoE Pilot

Building on its expertise leading the NSF Cybersecurity Center of Excellence, CACR is part of a team awarded a $3M 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.

During 2019, the pilot team primarily worked with the **National Ecological Observatory Network (NEON)**, an NSF major facility tracking ecological changes across North America. The pilot's objective during this time was to make improvements to NEON's operational cyberinfrastructure that would enable NEON to better serve the needs of the environmental research community. As a part of this broader effort, CACR staff assisted NEON in successfully developing and integrating a federated identity management solution for the portal, which is used by researchers to access the data collected by the various ground stations and sensor networks operated by NEON. Lessons learned during this effort will inform future work carried out by the pilot to help NSF projects solve cyberinfrastructure problems.

IS CYBERSECURITY FOR RESEARCH DIFFERENT?
ACT DIFFERENTLY
CENTER FOR APPLIED CYBERSECURITY RESEARCH
CYBERSECURITY FOR THE WORLD'S GREATEST RESEARCH
ResearchSOC
ResearchSOC

CLOCKWISE FROM TOP: Von Welch at Coalition for National Science Funding; Trusted CI poster at NSF large facilities workshop; Susan Sons at PEARC19

IRIS (RENCI)

CACR continued its partnership with the **Renaissance Computing Institute (RENCI)** on the **Integrity Introspection for Scientific Workflows (IRIS)** project. IRIS will automatically detect, diagnose, and pinpoint the source of unintentional integrity anomalies in scientific workflows executing on distributed computing infrastructure. CACR is supporting IRIS through expert guidance on cybersecurity and privacy challenges. RENCI is a partnership between the University of North Carolina–Chapel Hill, Duke University, and the city of Durham, N.C. RENCI leads a project allowing scientists to share and analyze data across institutional boundaries. The three-year project was funded by a $3M NSF grant.

Custos

The Custos project, a collaboration within PTI and led by PTI's **Cyberinfrastructure Integration Research Center (CIRC)**, will provide an innovative integration of major security capabilities needed by science gateways. These include identity management, secrets management for third-party resource integration, and group and sharing management for securely controlling permissions and broader access to the digital object science gateways. CACR provides cybersecurity consulting and input on best practices for this NSF-funded project.

ImPACT

CACR is contributing its cybersecurity expertise to a three-year, $3M project, funded by the National Science Foundation. The **Infrastructure for Privacy-assured CompuTations (ImPACT)** project, led by the Renaissance Computing Institute, will allow researchers to focus more fully on science by building a technology infrastructure that supports best practices in moving data, managing data, ensuring security, and preserving privacy.

The IRIS project uses machine learning techniques to monitor data at different points in the research workflow, identify unintentional errors, and trace their origins.

Log analysis training for Scholarship for Service students

CyberCorps SFSCon is a cybersecurity training and professional development event for the **CyberCorps Scholarship for Service (SFS)** students and alumni nationwide. CACR delivered a training and workshop on log analysis in this year's SFSCon in Pomona, California. This was attended by nearly 35 students of whom around 20 logged into the virtual machine for the workshop exercises.

Leading the conversation

At conferences and workshops across the country, CACR-led organizations set the pace in leading and shaping the national conversation about cybersecurity for research and education.

- For the first time, ResearchSOC presented a poster at the **National Science Foundation's large facilities workshop**, held April 2–4 at the Texas Advanced Computing Center (TACC) in Austin, Texas.

- In April, Von Welch hosted a poster presentation featuring Trusted CI and ResearchSOC at the **2019 Coalition for National Science Funding exhibition** "Building the Future" in Washington, D.C.

- In May at the **EDUCAUSE Security Professionals Conference**, ResearchSOC Co-P.I. Michael Corn, CISO at the University of California, San Diego, hosted the workshop, "Securing and Supporting Research Projects: Facilitation Design Patterns." In December, Corn hosted a three-day workshop, "Cybersecurity Engagement in a Research Environment," for researcher-facing cybersecurity professionals.

- Trusted CI's and ResearchSOC's leadership showed through at **PEARC19**, July 28–August 1:
  - Presented Trusted CI paper "Trusted CI Experiences in Cybersecurity and Service to Open Science"
  - Received the **PEARC19 Phil Andrews Award for Most Transformative Contribution** for SWIP's publication, "Integrity Protection for Scientific Workflow Data: Motivation and Initial Experiences"
  - Von Welch presented "A 5-year Vision for an NSF Cybersecurity Ecosystem"; CACR's Susan Sons led the birds of a feather session on "Securing Research CI"
  - Von Welch represented Trusted CI on the panel "Community Engagement at Scale: NSF Centers of Expertise"
  - ResearchSOC and Trusted CI presented posters

LEADING INDIANA TO A MORE SECURE FUTURE

ABOVE: CACR Security Matters cybercamp for high school students on IUPUI campus, June 2019

In 2019, CACR continued to increase its engagement with, and the value it brings to, the Hoosier state. CACR's initiatives helped to prepare county election officials to secure the 2020 vote, provide training for Indiana National Guard cybersecurity leadership, and educate Hoosier youth. CACR is also a driver for economic growth in South Central Indiana. CACR also contributes to Southeast Indiana's job growth, both directly and indirectly.

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 more than **$13M of new grant funds**. Over its lifetime, CACR has brought more than $44M award dollars to the South Central Indiana region. While methods of determining local economic impact vary, a Kelley School of Business estimate of the "ripple effect" is $2.10 of positive economic impact for every grant dollar spent, thus making **CACR's lifetime impact on the region more than $92M**.

Moreover, the Indiana Business Research Center at the 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 21 employees, an estimated **63 new jobs have been created** in the Bloomington and South Central Indiana area to date.

Securing the Hoosier vote

CACR's team of experts helped prepare election officials in all 92 Indiana counties for cybersecurity incidents related to the 2020 general election and beyond. At the **2020 Election Administrator's Conference**, the CACR team led a half-day "boot camp" and tabletop exercises in dealing with cybersecurity incidents, thanks to a $300K grant from Indiana Secretary of State Connie Lawson. The effort was a collaboration between CACR, OVPIT Information Security, and UITS Emergency Management and Continuity. The workshop also involved the new IU Cybersecurity Clinic with students helping in the training events.

TOP: CACR contributed to the state's STEM effort by participating in RISE, a two-week residential research camp at IU Bloomington. BOTTOM: In April, Director Welch presented a threat overview at Cyber Shield 19, a cybersecurity exercise that included 800 National Guard soldiers, airmen, and civilian participants from 40 U.S. states and territories.

TOP: CACR continues its partnership with NSWC Crane, a naval laboratory and field activity of Naval Sea Systems Command (NAVSEA). BOTTOM: High school students participate in the CACR Security Matters cybercamp on the IUPUI campus.

NSWC Crane and CACR: continuing the partnership

CACR and **NSWC Crane** continued their ongoing partnership that was recognized with the 2018 re-signing of the **cooperative research and development agreement (CRADA)**, a follow-on collaboration between NSWC Crane and CACR. The original agreement was executed in 2016. CACR and NSWC Crane continue to seek opportunities to increase collaboration and improve capabilities in the areas of software assurance and trusted artificial intelligence.

Conducting Cybersecurity Matters cybercamps

CACR also helped to ensure that tomorrow's Hoosier IT professionals are cybersecurity-smart. In June 2019, CACR held its **Security Matters cybercamp** for high school students on the IUPUI campus. 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 of Excellence for Women & Technology**.

Regional Bank Branch Ransomware
In this scenario, we are going to walk through an incident response plan for a ransomware incident at a regional bank branch. You will be assuming the roles of the Incident Response team. Please use the Incident Response plan to coordinate your response.
INDIANA UNIVERSITY BLOOMINGTON

LEADING IU TO HELP DRIVE DISCOVERY

During 2019, CACR provided new opportunities to further the university's research mission while serving as a key force in achieving IU's strategic objectives.

ABOVE: CACR hosted four cybersecurity incident response tabletop exercises for members of the IU M.S. in Cybersecurity Risk Management program and members of the IU cybersecurity club.

Fulfilling IU's strategic plan

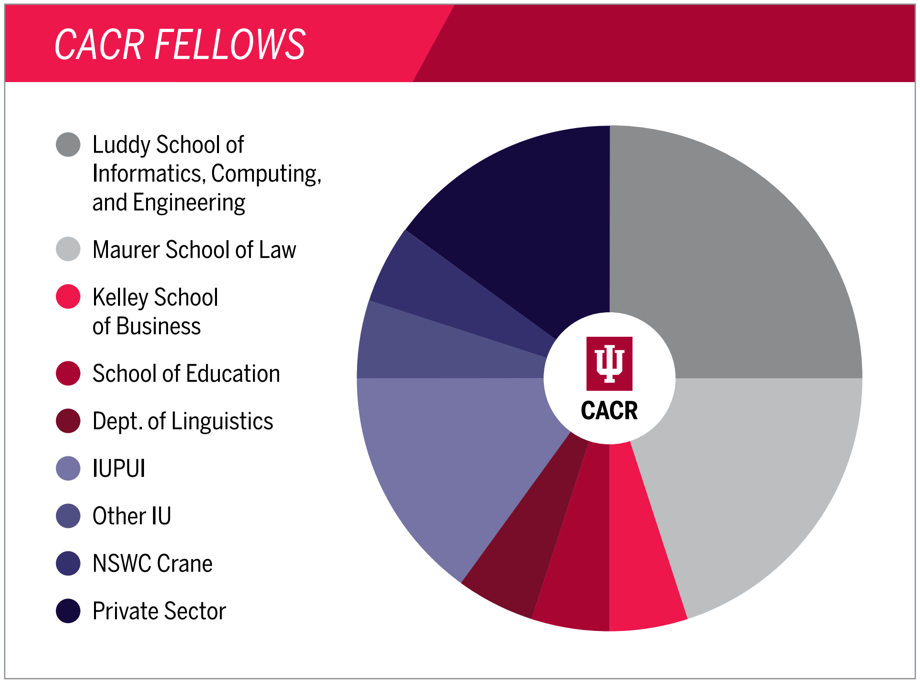
Through the growth and maintenance of key partnerships, CACR continued to meet the challenge presented in **IU's Bicentennial Strategic Plan** to "facilitate university-industry collaboration by identifying opportunities to work in areas such as cybersecurity with Indiana defense-related institutions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

Leading collaborations across IU

CACR's collaboration within PTI allows it to impact research computing broadly. CACR's awards continue to build collaborations across IU. The ResearchSOC award pulls together IU operational cybersecurity expertise with faculty from the Luddy School of Informatics, Computing, and Engineering. The SWIP project draws on Luddy's cybersecurity expertise. The PACT project draws on the expertise from the School of Education.

Evaluating the cybersecurity potential of artificial intelligence

CACR is leading a team piloting evaluation of a research prototype application designed to highlight collections of indicators, such as alerts, which represent attacker behavior during different types of cyberattacks, including novel attacker behavior. The **ASSERT application**, a collaboration with Ahmet Okutan and S. Jay Yang at Rochester Institute of Technology, uses theoretical-based measures to perform unsupervised learning from intrusion alerts across platforms. Over time, the system learns to build attack models, which may prove valuable for identifying attacks, determining their potential impact, and predicting future attacker behaviors. The team is determining if the prototype is a good fit for OmniSOC workflows and will be an improvement to enable broader adoption into 2020.



CACR Fellows represent a wide range of perspectives across IU and beyond.

A new role at IU: Executive Director for Cybersecurity Innovation (EDCI)

In May, IU appointed Von Welch executive director for cybersecurity innovation, a university-wide role responsible for leveraging IU's cybersecurity operational and research strengths in combination to address challenges faced across the nation. With this new role, Welch jointly reports to IU Vice President for Research Fred Cate and IU Vice President for Information Technology Brad Wheeler, while continuing his role as director of the CACR. "IU's Center for Applied Cybersecurity Research has a proven record of applying practical, interdisciplinary approaches to large-scale problems," said Cate, who is also a previous CACR director.

SecureMyResearch: safeguarding IU researchers' data

Securing research data, especially meeting new, stricter regulatory and other cybersecurity requirements, is becoming a challenge for both IU researchers and campus units that support research. To help them navigate this complex landscape, CACR, UITS Research Technologies, and OVPIT Information Security are partnering to reduce the cybersecurity burden on researchers while enabling improved cybersecurity for IU research projects. SecureMyResearch will enable them to concentrate on what they do best, namely world-class research, not unwelcome distractions. SecureMyResearch will leverage the combined expertise of IU's cybersecurity and compliance experts to weave data security and compliance into the institutional fabric, enhancing both regulated and unregulated data security with a new, workflow-based security framework developed by CACR.

Enabling secure health research

CACR continued to facilitate the HIPAA compliance effort for UITS. CACR worked with 14 new UITS systems and brought two to completion, passing a rigorous new institutional approval process CACR helped develop. In addition, CACR was a partner in **IU's Precision Health Initiative Grand Challenge** and played a key role in institutional HIPAA governance by facilitating the transition to new HIPAA privacy and security officers.

Strengthening IU's global partnerships

In May, CACR Director Von Welch joined a delegation to **Australian National University**, accompanying VPR Fred Cate and a contingent of six IU faculty and 12 students from both the IU cybersecurity program and Maurer School of Law. The centerpiece of the visit was a follow-on workshop to the 2018 "Making Democracy Harder to Hack" workshop, also co-hosted by IU and ANU and held in Washington, D.C. Welch met with colleagues at **ANU's Cyber Institute** as well as **Australia's National Computational Infrastructure** to further ongoing collaborations and CACR through its role as leader of the NSF Cybersecurity Center of Excellence.

FROM LEFT TO RIGHT:

S. Jay Yang (third from right), Rochester Institute of Technology professor and ASSERT developer, participated in the 2019 NSF Cybersecurity Technology Transition to Practice Workshop in Chicago.

CACR's Anurag Shankar presented "Risk Management 2.0" at IU's annual Statewide IT Conference. Von Welch also presented "CACR: Where it's been, where it's going, and why."

CACR Director Von Welch and VPR Fred Cate, plus IU faculty and students, take part in a delegation to Australian National University.

2019 CACR SPEAKER SERIES

cacr.iu.edu/events/speaker_series

The CACR 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.

January 31 | **Jonathan "J.J." Thompson**
A hard truth: Executives and boards don't care about cybersecurity (and why that's actually a good thing)
Thompson is founder and CEO of Rook Security.

February 7 | **Alex Halderman**
Cybersecurity and U.S. elections
Halderman is professor of computer science and engineering at the University of Michigan.

February 14 | **Alison Macrina**
Librarians at the forefront in the fight for privacy: Lessons from the Library Freedom Project
Macrina is founder and director of the Library Freedom Project.

65 AVERAGE ATTENDANCE (live/online)

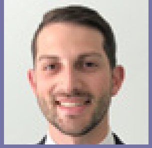
March 21 | **Gary Stoneburner**
Cybersecurity: Knowing why we're doing what it is we do
Stoneburner is a member of the senior professional staff of the Johns Hopkins Applied Physics Laboratory.

April 18 | **Susan Ramsey**
Cybersecurity for challenging environments: Complicated vs. complex systems and shared SOCs
Ramsey is a security engineer and risk assessor at the National Center for Atmospheric Research.

September 19 | **Andrew Korty**
Swift and reasonable action: A higher education CISO's perspective
Korty is CISO for Indiana University.

October 10 | **Nik Guggenberger**
Resolving the online tragedy
Guggenberger is executive director of the Information Society Project at Yale Law School.

November 7 | **Alan Mislove**
Measuring bias in social network ad targeting and delivery
Mislove is a professor and associate dean of undergraduate programs at the Khoury College of Computer Sciences.



November 14 | **Bryan Sacks**
"It's not me, it's you." Who said it best, the board or the CISO?
Sacks is CISO for the state of Indiana.

CACR thanks its partners and co-hosts: Center of Excellence for Women & Technology; Kelley School of Business; Luddy School of Informatics, Computing, and Engineering; Maurer School of Law; and Ostrom Workshop

leadership position addressing difficu
cybersecurity challenges through the
University's unique operational and
educational programs.
We welcome the opportur
collaborate with you.
Von Welch
vwelch@iu.edu | cacr.iu.edu
CYBERSECURITY
CYBERTECH MIDWEST 2019

CACR LEADERSHIP TEAM, STAFF, AND FELLOWS

ABOVE: In June, Director Von Welch presented a plenary at Cybertech Midwest while IU's booth property featured ResearchSOC

CACR's chief asset is its knowledgeable and dedicated administration, staff, fellows, and students. CACR prides itself on the professional diversity of its staff, each with unique skills and experiences that contribute to our expertise. CACR staff is made up of people from all disciplines, including computer science, informatics, accounting and information systems, criminal justice, law, organizational behavior, and public policy.

CACR LEADERSHIP TEAM

CACR Director and IU Executive Director for Cybersecurity Innovation **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** focuses on information security program development and governance, cybersecurity assessment design and conduct, legal and regulatory impact on information security and cyber resilience, evidence-based security, and innovative defenses.

Chief Security Analyst **Mark Krenz** focuses on cybersecurity operations, research, and education. He has more than two decades of experience in system and network administration and serves as the CISO for the ResearchSOC and Deputy CISO of Trusted CI.

Senior Security Analyst **Anurag Shankar** provides leadership in regulatory compliance (HIPAA, FISMA, and DFATS) and cybersecurity risk management. He has over two decades of experience in providing research computing services and building HIPAA-compliant solutions for biomedical researchers.

Senior Project Manager **Kelli Shute** supports Trusted CI, ResearchSOC, and our election security engagement with the state of Indiana. She has more than 15 years of experience leading project teams, primarily in the private sector.

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. She serves as information security officer for Open Science Grid and deputy director of the ResearchSOC.

FROM TOP: ResearchSOC staff; Trusted CI Fellows at the 2019 NSF Cybersecurity Summit; Trusted CI staff at NSF Cybersecurity Summit

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 Cimmer | Events & Communications Manager
Adrian Crenshaw | Senior Security Analyst
Austin Cushenberry | IT Support Specialist
Josh Drake | Senior Security Analyst
Will Drake | Senior Security Analyst
Tom Edelberg | Research Associate
Ryan Kiser | Senior Security Analyst
Tori Richardson | Senior Administrative Assistant
Ranson Ricks | Senior Project Manager
Scott Russell | Senior Policy Analyst
Zalak Shah | Senior Security Analyst
Mike Stanfield | Senior Security Analyst

TRUSTED CI FELLOWS

Trusted CI Fellows empower members of the scientific community with basic knowledge of cybersecurity and the understanding of Trusted CI's services, and then have them serve as cybersecurity liaisons to their respective communities.

Shafaq Chaudhry | University of Central Florida
Matias Carrsco Kind | National Center for Supercomputing Applications
Gabriella Perez | University of Iowa
Aunshul Rege | Department of Criminal Justice at Temple University
Chrysafis Vogiatzis | North Carolina A&T State University
S. Jay Yang | Rochester Institute of Technology

FELLOWS AND KEY LIAISONS

CACR has more than a dozen Fellows. Each one brings unique insights and connections to the center, allowing it to capitalize on the interdisciplinary strengths of IU and the broader community. Fellows represent a wide range of perspectives, including law, policy, ethics, and informatics.

Mark Bruhn | IU former Associate Vice President for Assurance and Public Safety
Fred H. Cate | Maurer School of Law
L. Jean Camp | Luddy School of Informatics, Computing, and Engineering
Damir Cavar | College of Arts and Sciences, Department of Linguistics
Robert Cowles | Brightlite Information Security
Rachel Dockery | Maurer School of Law
Arjan Durressi | Department of Computer and Information Science, IUPUI
David P. Fidler | Maurer School of Law
Grayson Harbour | Faegre Baker Daniels LLP, Indianapolis
Daniel Hickey | School of Education
Raquel Hill | Luddy School of Informatics, Computing, and Engineering
Apu Kapadia | Luddy School of Informatics, Computing, and Engineering
Nicholas Multari | Pacific Northwest National Lab, Washington
Steven Myers | formerly of Luddy 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 | Luddy School of Informatics, Computing, and Engineering
Xukai Zou | Department of Computer Science and Information Science, IUPUI

OTHER IU CYBERSECURITY COMMUNITY MEMBERS

IU Office of the Associate Vice President for Information Security | protect.iu.edu/online-safety
GlobalNOC | globalnoc.iu.edu
Hamilton Lugar School of Global and International Studies | hls.indiana.edu
IU Cybersecurity Risk Management Program | cybersecurity.iu.edu
Kelley School of Business | kelley.iu.edu
Luddy School of Informatics, Computing, and Engineering | sice.indiana.edu
Maurer School of Law | law.indiana.edu
OmniSOC | omnisoc.iu.edu
Ostrom Workshop | ostromworkshop.indiana.edu
REN-ISAC | ren-isac.net

CENTER FOR APPLIED
CYBERSECURITY RESEARCH

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

cacr.iu.edu

*CACR's work is funded by the IU Office of the Vice President for Information Technology, the IU Office of the Vice President for Research, the IU Office of the President, the Department of Homeland Security, and the National Science Foundation (grants **1547272, 1642070, 1659367, 1840034, 1920430**). None of the opinions expressed in this report should be assumed to represent the opinions of funding entities.*

CACR is a research center affiliated with the Indiana University Pervasive Technology Institute.