Center for Applied Cybersecurity Research

2015 Annual Report and Strategic Plan (2015-2020)

From the CACR Director

Dear friends,

The cybersecurity landscape continues to challenge businesses, universities, government, and society as a whole. This last year brought high-profile attacks with increasing sophistication and impact. Well-publicized breaches in the commercial sector, government, and higher education concern a growing proportion of the population.

In my first year as director of CACR, leading efforts to address these challenges has been gratifying. A common theme in these attacks is the gap between leading edge cybersecurity research and implementation. CACR continues its philosophy of applied research, bridging this gap by combining research from across the disciplines of technology, law, policy, economics, and human factors to advance the state of practice in cybersecurity.

CACR exists as an Indiana University-wide center and as such acts to improve cybersecurity across Indiana and the nation. As part of the Pervasive Technology Institute (PTI), it works in collaboration with other PTI centers "to improve the quality of life in the state of Indiana and the world through novel research and innovation and service delivery in the broad domain of information technology and informatics."

CACR leads the Center for Trustworthy Scientific Cyberinfrastructure, a multi-organizational effort funded by the National Science Foundation (NSF) to secure open science across the more than $7 billion of research it funds. This research is critical to advancing our knowledge and feeding the innovations that drive our economy. We've worked with over 70 NSF projects through one-on-one engagements, training, or participation in the annual NSF Cybersecurity Summit we organized and hosted.

Our work as part of the Department of Homeland Security Software Assurance Marketplace is improving the security of the nation's software. As software is becoming nearly ubiquitous and more personal, strengthening our assurance in software security is increasingly critical – and CACR is seeking to address not only the technical challenges to providing that assurance, but also the incentives and usability issues for making that assurance part of everyday software development.

We are also happy to announce that, because of efforts such as these and many others across Indiana University, IU's designation as a NSA/DHS Center of Academic Excellence in Information Assurance Education and Research has been renewed through 2021.

Cybersecurity will continue to challenge us because the threats continue to evolve. CACR will continue to evolve to rise and meet tomorrow's threats. It's a great pleasure to lead this organization with a world-class leadership team, staff, and contributing researchers from across Indiana University.

About CACR

The Center for Applied Cybersecurity Research was established by Indiana University in 2003 to provide the nation with leadership in applied cybersecurity technology, education, and policy guidance. Properly balancing public needs, homeland security concerns, and individual privacy rights is fundamental to CACR's mission. The center has been named a National Security Agency (NSA)/Department of Homeland Security (DHS) National Center of Academic Excellence in both Information Assurance Education and Information Assurance Research.

CACR is distinctive in interweaving technical and policy expertise. The Center draws on Indiana University's wide range of scholarly expertise in computer science, informatics, accounting and information systems, criminal justice, law, organizational behavior, public policy, and other disciplines, as well as the extensive practical cybersecurity experience of its operational units.

Building on this foundation, CACR has achieved a number of successes over the past year:

- Organizing the National Science Foundation's Cybersecurity Summit for Large Facilities and Cyberinfrastructure
- Winning the ISE North America Project of the Year Award in the Academic/Public Sector Category for the Department of Homeland Security Software Assurance Marketplace Project
- Recertifying Indiana University as a Center of Academic Excellence in Information Assurance Education and Research
- Leading a faculty group representing six Indiana University schools in the development of a white paper for the Department of Defense's Minerva social science research initiative

As a result, CACR has risen to a position of prominence in national and global cybersecurity conversations. CACR's mission and vision are ambitious but achievable. They challenge CACR—and Indiana University—to identify and address the most difficult cybersecurity problems facing public and private communities alike. And they invite continued collaboration to foster greater innovation and creativity.

CACR is distinctive in interweaving technical and policy expertise.

CACR's mission is to advance the state of cybersecurity practice, interdisciplinary research, and understanding in order to serve Indiana University, the state of Indiana, and our national and global communities. Ultimately, CACR envisions becoming a global leader and partner of choice for addressing the multidisciplinary cybersecurity challenges of the modern world.

Since its origination in 2003, CACR has garnered more than $16 million in direct research funding from a variety of sources, including Lilly Endowment, Inc., the National Science Foundation, the Department of Energy, and the National Institutes of Health. Currently, the Center is managing approximately $5.1 million in research funding from the National Science Foundation and the Department of Energy.

Major impacts

CACR is leading the nation in applied cybersecurity technology, education, and policy guidance.

The Center for Trustworthy Scientific Cyberinfrastructure (CTSC)

trustedci.org

CTSC is comprised of cybersecurity experts who have spent decades working with science and engineering communities and have an established track record of usable, high-quality solutions suited to the needs of those communities. The team draws from best operational practices and includes leaders in the research and development of new methodologies and high-quality implementations.

Funded by the National Science Foundation, the mission of CTSC is to improve the cybersecurity of NSF science and engineering projects, while allowing those projects to focus on their scientific endeavors.

This is accomplished through one-on-one engagements with projects to address their specific challenges; education, outreach, and training to raise the state of security practice across the scientific enterprise; and leadership on bringing the best and most relevant cybersecurity research to bear on the NSF cyberinfrastructure research community.

Additionally, the CTSC hosts the annual NSF Cybersecurity Summit, bringing the NSF and research communities together to build understanding of the information assets that enable science, while providing the community with a forum for education, sharing experiences, building relationships, and establishing best practices.

XSIM

The Advanced Identity Management for Extreme-Scale Scientific Computing (XSIM)

XSIM has a three-year plan to engage with communities and examine existing implementations, determining how they interact with their users and resource providers, and capturing that in a coherent model. Subsequently it will develop supporting software, both to validate the model it develops and advance the state of practice. The focus on collaboration within identity management was chosen due to its importance to the scientific community, the limited number of collaboration-resource provider relationships (making it a reasonable area for progress), and the fact that much applied research has been done in this specific area (making it ready for a formal model). All project results will be open and freely available.

This project is funded under the DOE Scientific Collaboration at Extreme-Scale program.

SWAMP

The Software Assurance Marketplace (SWAMP)

continuousassurance.org

The SWAMP was developed to make it much easier to regularly test the security of applications and provide an online laboratory for inventors to build stronger software assessment tools. Comprehensive testing is often complicated and challenging, as it requires the use of several disparate tools with no central means of managing the process.

Funded by the Department of Homeland Security, the SWAMP is a no-cost, high-performance, centralized cloud-computing platform that includes an array of open-source and commercial software security testing tools, as well as a comprehensive results viewer to simplify vulnerability remediation.

A first in the industry, the SWAMP also offers a library of applications with known vulnerabilities, enabling tool developers to improve the effectiveness of their own static and dynamic testing tools.

Created to advance the state of cybersecurity, protect critical infrastructures, and improve the resilience of open-source software, the SWAMP integrates security into the software development lifecycle and keeps all user activities completely confidential. This project won the 2014 Information Security Executive North America Project of the Year award in the Academic/Public Sector category, an honor only bestowed on those organizations that have undertaken many of security's most difficult challenges in order to better protect their institutions and bring advancement to the industry.

NSA/DHS National Center of Academic Excellence certification

In 2014, the National Security Agency (NSA) and the Department of Homeland Security (DHS) designated Indiana University as a National Center of Academic Excellence in Cyber Defense Research (CAE-R) through academic year 2021. A letter sent to CACR noted that the Center's "ability to meet the increasing demands of the program criteria will serve the nation well in contributing to the protection of the National Information Infrastructure."

IU was initially certified as a Center for Academic Excellence in Information Assurance/ Cyber Defense Education in 2007 and as a Center for Academic Excellence Information Assurance/Cyber Defense Research in 2008 (the first year this certification was offered). IU is one of just a handful of universities to have dual designations spanning more than one campus.

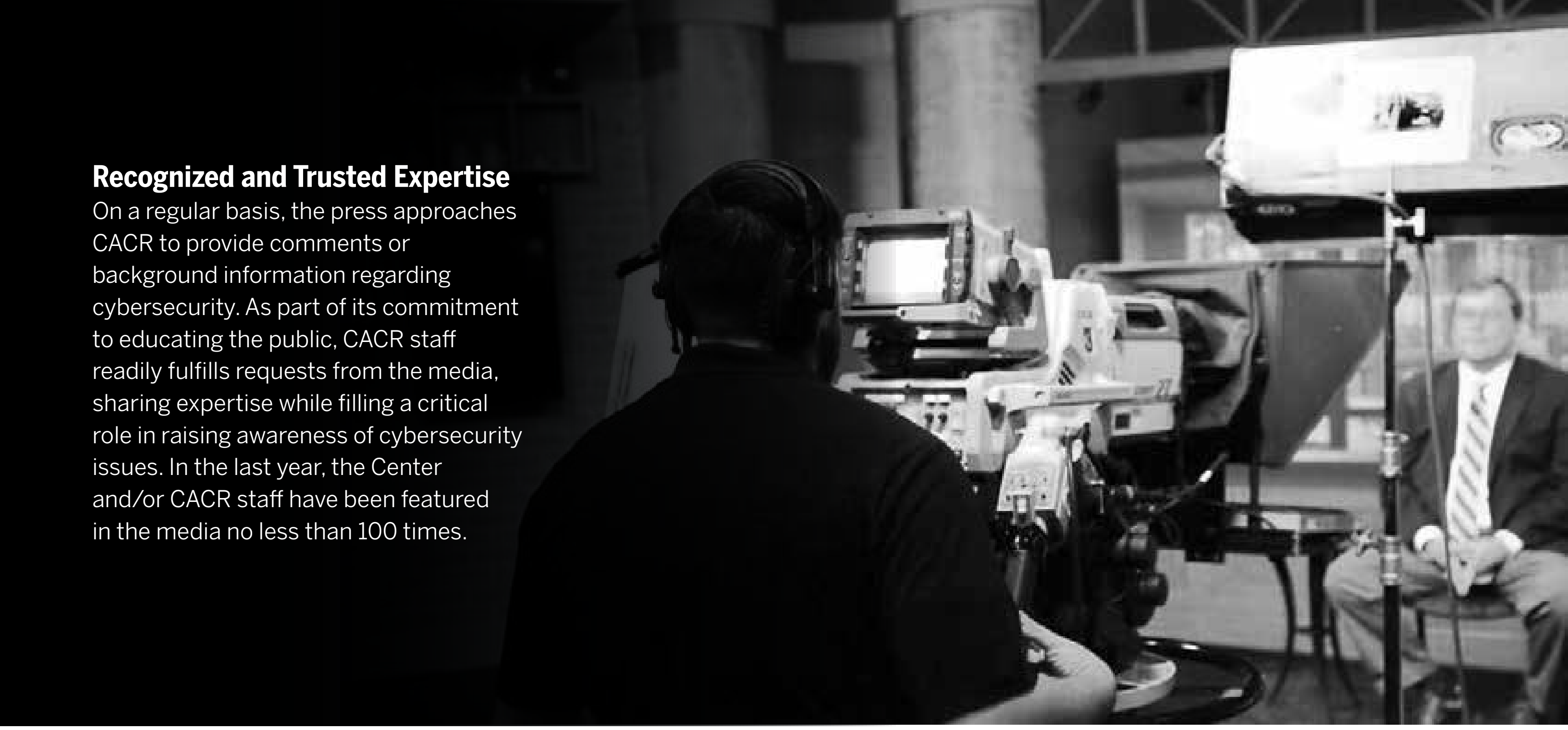
IU's Center for Applied Cybersecurity Research coordinated the application process, working closely with faculty and staff at the IU School of Informatics and Computing, both on the IU Bloomington and Indiana University-Purdue University Indianapolis (IUPUI) campuses.

The NSA created the Center for Academic Excellence program in 1998 as a way to reduce vulnerability in the US information infrastructure by promoting higher education and research in cybersecurity, thereby fostering a workforce of well-trained professionals. In fact, students attending Center for Academic Excellence-designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program.

A letter sent to CACR noted that the Center's "ability to meet the increasing demands of the program criteria will serve the nation well in contributing to the protection of the National Information Infrastructure."

InCommon Steering Committee appointment

Identity and authentication are critical foundational layers to cybersecurity. In the higher education community, InCommon, operated by Internet2, provides a secure and privacy-preserving identity federation for research and higher education. This past year, CACR Director Von Welch was appointed to the InCommon Steering Committee as an advisor representing the research community, a newly created position recognizing Welch's leadership in securing our national research by leveraging federated identity.



Recognized and Trusted Expertise

On a regular basis, the press approaches CACR to provide comments or background information regarding cybersecurity. As part of its commitment to educating the public, CACR staff readily fulfills requests from the media, sharing expertise while filling a critical role in raising awareness of cybersecurity issues. In the last year, the Center and/or CACR staff have been featured in the media no less than 100 times.

Educating the nation on CYBERSECURITY

CACR's mission is to advance the state of cybersecurity practice, interdisciplinary research, and understanding in order to serve Indiana University, the state of Indiana, and our national and global communities. A large part of this is done through general outreach and communication efforts, as well as events.

Security Matters

Security Matters is a service of CACR. The series – initially 12 episodes – has addressed specific security threats or vulnerabilities through brief audio segments on WFIU along with simple how-to video segments at securitymatters.iu.edu. In the coming year, the Security Matters project will undergo a transformation, but the CACR is dedicated to ensuring that the project remains a source of information and education for the public regarding security threats and vulnerabilities.

Outreach efforts

One of the features of the Center's work is to focus on security challenges in context. This is done through outreach with the various communities the Center serves. In the past year, the Center has provided outreach in a number of ways, the most notable being:

- Acted as a state of Indiana DHS Summit assistant and panelist
- Delivering the keynote address at the 2015 Secure and Resilient Cyber Architectures Invitational (Perceptions and Barriers to Resilience: A Newcomer's Perspective)
- Presenting at the Internet2 Global Summit (Trustworthy Computational Science: A Multi-decade Perspective)
- Leading the NewGuard Project
- Directing the Internet Civil Engineering Insitute

CACR Summit

CACR has been bringing together leading visionaries in the areas of applied cybersecurity technology, education, and policy in an annual Cybersecurity Summit since 2010. During this one-day event, attendees discuss the proper balance of public needs, homeland security concerns, and individual privacy rights. Featured speakers have included Thomas Parenty (founder, Parenty Consulting Ltd. and advisor to foreign firms in China on computer security), Richard Bejtlich (Chief Security Officer, Mandiant), Christopher Soghoian (Chief Technologist and Policy Analyst, ACLU Speech, Privacy, and Technology Project), Suzanna Spaulding (Undersecretary for the National Protection Programs Directorate, Department of Homeland Security), Sharon M. Jackson (National Security Chief, Indianapolis US Attorney's Office), and Doug Maughan (Director of Cyber Research and Development, US Department of Homeland Security). Past topics have included Cybersecurity in Higher Education, Cyberwar, Is the US Responding to the Perception or Reality of China's Cyberthreats?, and Global Issues, Local Needs. The 2015 CACR Cybersecurity Summit will focus on Privacy and Risk Management. Additional information about the Summit can be found at: https://uits.iu.edu/cybersecurity-summit.

CACR brings together leaders in Cybersecurity from across the country

Cyber War, Cyber Peace, Stones, and Glass Houses
those who live in glass houses should not throw stones

Security Seminar Speaker Series

This past year marked the fifth year of the Security Seminar Speaker Series. Held at least monthly, these presentations invite cybersecurity professionals from all over the country to give talks on their individual areas of expertise. These talks are open to all interested students, faculty, and staff, and are offered at IUPUI via live stream. The 2014-2015 Speaker Series featured the following experts speaking on the listed topics:

Fostering Innovation in Cybersecurity
Anita Nikolich, Program Director for Cybersecurity in the Division of Advanced Cyberinfrastructure,
National Science Foundation

Internet Voting: Both Sides of the Story
Alex Yasinsac, Dean
University of South Alabama's School of Computing

Meatball Surgery: Operational Information Security at a Large Higher Education Institution
Andrew Joseph Korty, Information Security Officer
Indiana University

All Your SSL Are Belong to Us
Vitaly Shmatikov, Associate Professor of Computer Science
University of Texas at Austin

Cyber Threat Information Sharing
Kim Milford, Executive Director
REN-ISAC

CACR Director's Update
Von Welch, Director,
Center for Applied Cybersecurity Research
Indiana University

Reasoning Cryptographically About Knowledge
Rafael Pass, Associate Professor,
Cornell University Department of Computer Science

Insuring Cyber Risks
Christopher French, Visiting Assistant Professor of Law
Penn State Law

Hidden Gems: Automated Discovery of Access Control Vulnerabilities in Graphical User Interfaces
Engin Kirda, Professor of Computer Science
Northeastern University

Provable Privacy in the Wild: Challenges and Open Questions
Ashwin Machanavajjhala, Assistant Professor
Department of Computer Science
Duke University

NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

Through the Center's work with the CTSC, CACR has planned and executed the past two NSF Cybersecurity Summits for Large Facilities and Cyberinfrastructure. The NSF cyberinfrastructure ecosystem presents an aggregate of complex cybersecurity needs (e.g., scientific data and instruments, unique computational and storage resources, complex collaborations) as compared to other organizations and sectors. This community has a unique opportunity to develop information security practices tailored to these needs, as well as break new ground on efficient, effective ways to protect information assets while supporting science. The Summit brings together leaders in NSF cyberinfrastructure and cybersecurity, allowing them to annually work toward building a trusting, collaborative community and seriously address the community's core cybersecurity challenges. Viewed as critical to cybersecurity, at least one NSF solicitation has made attendance a mandatory component of the award.

The Center has continued to work as a connection between the operational, practical, and academic at the university.

Maximizing IU's Cybersecurity Impact

As President McRobbie envisioned in 2003, CACR operates at the intersection of the university's academic, research, operational, and policy cybersecurity communities. The university's recognized strengths include:

- The Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)
- Highly ranked programs at the Maurer School of Law, School of Informatics and Computing, and Kelley School of Business
- Outstanding technical research communities such as the Pervasive Technology Institute, Network Science Institute, and the Ostrom Workshop
- Centers in specialized areas that benefit cybersecurity, including the Center for Intellectual Property Research, Cyberinfrastructure for Network Science Center, Randall L. Tobias Center for Leadership Excellence, Center on Congress, Center on American and Global Security, and Poynter Center for the Study of Ethics and American Institutions
- Strong operational security programs including the University Information Security Office, the University Privacy and Information Policy Office, and the Global Research Network Operations Center

CACR bridges technical specialties in cybersecurity with business, law, and the behavioral disciplines. This has further allowed the university to link with the industry, government, and wider world.

The Center has continued to connect the operational, practical, and academic at the university. During this past year, it has participated in many activities to promote this, including:

- Undertaking strategic planning
- Sponsoring students to Tapia via SOIC/Lamara Warren
- Leading an interdisciplinary coalition of IU researchers to submit a white paper for the DOD Minerva Initiative, a significant step towards developing the cybersecurity research community, bringing together IU's strengths across schools
- Assisting with an undergraduate research project on cryptography that involved secure, wireless communication for a portable medical device (and required CACR background information related to encryption and authentication)

Over the next five years, CACR will pursue three strategic initiatives:

Lead

Increase

Advance

Lead

collaborative activities to enable a more cohesive, more impactful cybersecurity community at Indiana University

CACR has a unique opportunity to lead, coordinate, and facilitate cybersecurity activities for the university. Through the following actions, CACR will strive to benefit from and improve the capabilities of all parts of the university:

- 1.1: In partnership with all interested university entities, create a website to serve as a single online portal to the university's cybersecurity expertise, activities, and educational opportunities
- 1.2: Propose a cybersecurity Grand Challenge in furtherance of the university's Bicentennial strategic plan
- 1.3: Support the fulfillment of Grand Challenge proposals by other university entities
- 1.4: Focus CACR's annual summit on risk management and privacy issues of interest to university, as well as local and national communities
- 1.5: Lead and facilitate the development of a vibrant, system-wide cybersecurity community through faculty relationships, collaborative academic programs, and informative programs for the public

In all of its activities, CACR commits to addressing topics of broad interest that present significant opportunity to conduct collaborative work. Privacy, risk management, governance, big data, information sharing, and leadership meet these criteria. Through ongoing strategic planning activities, CACR will incorporate additional topics that appeal to the university community.

Increase

CACR's impact on the state of Indiana

CACR has a number of existing initiatives that benefit the state of Indiana, such as the annual CACR Summit, speaking at local and state events, and the Security Matters educational initiative. More direct benefit could be achieved through collaboration with other state entities that are working on cybersecurity, bringing CACR expertise on trustworthy infrastructure, privacy, and software assurance – expertise developed at the national level, through federal funding – to benefit the state of Indiana. The following actions will enable CACR to increase its visibility and leadership at the state level:

- 2.1: Implement an active CACR fellows program that promotes collaboration among academic disciplines and government, corporate, non-profit, and other communities
- 2.2: Expand collaborations to increase CACR's value to the state of Indiana by including one or more of the Indiana National Guard, Office of Information Technology, Indiana Information Sharing and Analysis Center, the Naval Surface Warfare Center Crane Division, and other state entities
- 2.3: Continue to strengthen and focus CACR's outreach and education programs to benefit populations in the state of Indiana

Advance

CACR to address healthcare cybersecurity issues

Healthcare is a strategic priority for Indiana University; it is identified as principle of excellence in the Indiana University Bicentennial Strategic Plan and as a Grand Challenge in Indiana University's Strategic Plan for Information Technology. The healthcare field can readily benefit from CACR's strengths, and it presents many of the most pressing cybersecurity issues for the coming generation to study and address.

Information-related issues include the use of cloud services, the digitization of medical records, privacy and security, and big data analytics. Governance, economics, legal, and policy issues are intertwined in federal laws and regulations. And cybercrime is a growing concern as groups target health information, weak corporate security practices, and underdeveloped risk management strategies. In short, there is a real market need for CACR's cybersecurity skills and expertise. With the addition of HIPAA consulting services, CACR will have a direct and measurable impact on healthcare cybersecurity.

The following actions will enable CACR to establish itself as a leader in the field of healthcare security:

- 3.1: Offer consulting services on the Health Insurance Portability and Accountability Act (HIPAA) and integrate related knowledge into other CACR projects
- 3.2: Collaborate with university entities to pursue funding to secure health information and/or infrastructure
- 3.3: Collaborate with university researchers and practitioners to lead at least one interdisciplinary research proposal

Through these initiatives, the Center will continue to cement its status as a world leader in the academic and research sides of cybersecurity.

Leadership

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.

Senior Fellow and founding Director **Fred H. Cate** specializes in information security law and policy issues and is routinely called upon to testify before congressional committees; speak before professional, industry, and government groups; and comment on cybersecurity-related stories in the news.

Deputy Director **David Delaney** is also a member of faculty of the Indiana University Maurer School of Law, where he specializes in constitutional, statutory, regulatory, and international law on issues involving cybersecurity, critical infrastructure protection, and intelligence matters.

Associate Director **William Barnett** is senior manager for life sciences in the UITS Research Technologies office, and director of the Advanced IT Core in the IU School of Medicine. Dr. Barnett has also recently been named the first Indiana CTSI and Regenstrief Chief Research Informatics Officer.

Associate Director **Mark Bruhn** is Indiana University's associate vice president for assurance and public safety.

Associate Director **Scott Orr** is an instructor in Network Security and System Administration at IUPUI.

Administrative Director **Leslee Cooper** has over two decades of accounting and financial management experience.

Staff

CACR staff help manage daily operations such as administrative, management, external relations support, as well as security and policy analysis.

Randy Heiland,
Senior Systems Analyst/Programmer

Craig Jackson,
Senior Policy Analyst

Ryan Kiser,
IT Specialist

Mark Krenz,
Lead Security Analyst

Sarah Portwood,
Executive Assistant to Fred H. Cate

Anurag Shankar,
Senior Security Analyst

Susan Sons,
Senior Systems Analyst

Amy Starzynski Coddens,
Education, Outreach and Training Manager

Suzi Pointer,
Senior Administrative Assistant

Fellows

CACR sponsors nearly a dozen fellows representing a wide range of perspectives, including law, policy, ethics, and informatics.

Fred H. Cate, Maurer School of Law
L. Jean Camp, School of Informatics and Computing
Jake Chen, School of Informatics and Computing (IUPUI)
Arjan Durress, Department of Computer and Information Science (IUPUI)
Andrew Proia, CACR, Information Security Law & Policy
David P. Fidler, Maurer School of Law
Mailyn Fidler, Oxford University
Apu Kapadia, School of Informatics and Computing
Scott J. Shackelford, Kelley School of Business
Chris Soghoian, ACLU
Xiaofeng Wang, School of Informatics and Computing
Gianpaolo Russo, CACR, Global Cybersecurity
PolicyXukai Zou, Department of Computer Science (IUPUI)

Acknowledgements

CACR can only do the work that it does thanks to the generous funding it receives from the OVPIT, IU Office of the President, NSF, DHS, and DOE.

CENTER FOR APPLIED
CYBERSECURITY RESEARCH

INDIANA UNIVERSITY
Pervasive Technology Institute