UNIVERSITY OF DELAWARE | Cybersecurity Initiative

# University of Delaware Cybersecurity Initiative Research Grant (UD CSI)

## 2015/2016 GRANT GUIDELINES

Cybersecurity Initiative
110 Du Pont Hall
Newark, DE 19716
*Phone:* (302) 831-1510
*Email:* cybersecurity@win.udel.edu

## UD CYBERSECURITY INITIATIVE (UD CSI) MISSION STATEMENT

The mission of the University of Delaware Cybersecurity Initiative (UD CSI) is to establish UD as a center of excellence in cyber security that encompasses research, education, workforce training and development, and promotes partnerships among the government, private and academic communities. UD CSI has a strategic focus to serve as the cyber security hub for corporate America.

Recognizing the constant and ever evolving threats to our nation's corporate community, the University of Delaware Cybersecurity Initiative is designed to address two significant challenges. First, UD CSI will produce unbiased research, best practices and standard protocols for optimal security so that every type and size of business can protect itself. Second, UD CSI will dramatically expand the pipeline of skilled cybersecurity workers that our nation needs now and in the future.

UD is the ideal location for a cybersecurity hub. Located halfway between New York City and Washington, DC, the University can help make the essential connections between the corporate community and the military and intelligence community. Also, Delaware is the legal home of more than 1 million corporations and a highly regarded court system, so legal questions in the evolving field of corporate cybersecurity will be adjudicated in Delaware. Finally, UD already has the expertise in computer engineering, computer science, corporate law and public policy.

UD CSI is developing programs through relationships with the U.S. Army, the Delaware National Guard, JPMorgan Chase, MITRE Corporation, Morgan Stanley, Bank of America, Raytheon, DuPont, GE, IBM, The Chertoff Group, Battelle Memorial Institute, Delaware State University, Delaware Technical Community College and others.

## CYBERSECURITY BACKGROUND

America's critical infrastructure in continually under cyber-attack in the form of exfiltration of intellectual property in the form of break-in's, denials of service/DOS, eavesdropping, man-in-the-middle, data modifications and any other exploit that the human imagination can develop.  According to Computer Security Institute's most current annual survey:

While cybersecurity incidents are multiplying in frequency and cost, the cyber risk management programs of most organizations do not rival the sophistication and persistence of aggressors.  Experts conclude that few organizations today adequately address employee and insider vulnerabilities, nor do they assess the security practices of third-party partners and their supply chain partners. What is needed is research guidance and educational programs to prepare the workforce on how to invest strategically in cybersecurity and ensure that it is incorporated in business strategies, and cognitive human behavior. Experts agree there need to be a shift in thinking around cybersecurity as an "IT" problem to one that spans the entire enterprise as a systems approach.

## PURPOSE OF UD CSI RESEARCH GRANTS

The Office of the Provost established this effort for the purpose of cultivating multidisciplinary cybersecurity exploration at the University of Delaware as an essential component in contributing to the existing and future cybersecurity workforce. This effort requires the coordination of non-technical educational applications with core technical understanding. The purpose of this grant program is to support work that complements and extends the development of both technical and nontechnical cybersecurity in a collaborative intercollege spirit.

## EILIGIBILITY FOR UD CSI RESEARCH GRANTS

UD CSI will support high quality multidisciplinary research projects by early-career, untenured, tenure-track and tenured faculty. UD faculty are encouraged to submit proposals for research funds to examine issues in all interdisciplinary aspects of cybersecurity with emphasis on curriculum development, financial, managerial and behavioral topics. Preference will be given to merit-based projects with interdisciplinary/multidisciplinary collaboration, technology/engineering partnership and/or industry connection. Only one award may be received per calendar year.

Possible avenues of inquiry are:

- Tools for institutions to evaluate their cybersecurity risk and their risk management capabilities and management approaches to identify, measure, mitigate and monitor risks.
- Methods to develop and evaluate processes for gathering, analyzing and sharing information with each other during cyber incidents.
- Governance mechanisms for providing executives with accurate and timely information about risks and ability to mitigate them to prioritize our resource allocations and inform the board of directors.
- Guidance on the tone at the top, how to build a security culture, and creating governance processes to ensure ongoing awareness and accountability and ensuring reports to senior management and corporate boards are meaningful and timely with metrics on the institution's vulnerability to cyber risks and potential business impacts.
- Service provider strategies that focus on technology service providers' ability to respond to growing cyber threats and vulnerabilities.
- Ways for companies to build upon existing relationships with law enforcement and intelligence agencies to share information on the growing cybersecurity threats and response techniques.
- Development of a Cybersecurity Certificate Program/ Education Programs some ideas include but are not limited to a focus on multi-disciplinary programs, SCADA courses, NIST standards, Cyber Hygiene for Students and Small Businesses etc.
- Healthcare Cybersecurity
- Development of Cybersecurity Table Top Exercise
- Development of Cybersecurity Case Study
- Cybersecurity Architecture, Analytics and visualization tools
- Current state of Threats/ Lessons Learned
- Meteorological Flood Forecasting and Monitoring
- Emerging Cyber Threats / Emerging Technologies
- AUVAC Mapping
- Ethics, Governance and Criminal Justice
- Unmanned Undersea Vehicle Detection and Classification Harbor Protection

- Intrusion Prevention and Automated Protection
- Social Engineering
- Autonomous Underwater Vehicle Data Stream Protection
- Cyber law
- Cybersecurity Wind Turbine Data Stream Protection
- Security Information Management
- EV to G data protection
- Government and Industry Cooperation Models
- Legislative / Regulatory Affairs in Cyber law
- Risk Management
- Meteorological, Environmental Remote Sensing Analysis
- Policy and Compliance
- Cyber Threat Intelligence / Information Sharing
- Intergovernmental / Inter-agency and International Cooperation
- Critical Infrastructure & Operational Technology Security
- High Performance Computing and Big Data Security
- Mobile Device and Application Management
- Wireless and Mobile Security
- Cloud Security
- Neural Network Analysis
- Cryptography
- Identity/Access Management and Biometric Authentication
- Malware and Hardware Security
- IT Forensics / Digital Forensics
- Application Security / Enterprise Governance
- Information Protection Technologies / Encryption
- Incident Response Management
- Advanced Persistent Threats / Advanced Evasive Techniques
- Supply Chain Security
- SCADA I Industrial Control Systems
- Endpoint Security
- Data Mining
- Digital cybercrime investigation techniques
- Digital Privacy
- Cyber Insurance Studies

## AWARD ADMINISTRATION

University of Delaware Cybersecurity Initiative research grants are awarded on the basis of eligibility and merit and administered by the UD Cybersecurity Initiative. Proposals are screened for eligibility and each proposal must have a match from the Dean of the College. Evaluations of merit and award final decisions are made by a committee appointed by Dr. Starnes Walker, Founding Director - UD Cybersecurity Initiative.

The university's patent, copyright, and publication policies, which can be found in the Handbook for Faculty (http://facultyhandbook.udel.edu/), apply to research conducted under a UD CSI grant. University policy and federal law (45 CFR 46) require that all research involving living human subjects be reviewed and approved by an Institutional Review Board (IRB). In addition, federal regulations require that all use of non-human vertebrate animals in research, teaching, and testing follow established guidelines and be reviewed and approved by an Institutional Animal Care and Use Committee (IACUC), which is constituted according to the Public Health Service Policy on Humane Care and Use of Laboratory Animals. Additional information is available at http://www.udel.edu/research/researchers/policies-forms.html.

## PROPOSAL BUDGET

The typical UD CSI project budget is $30,000 of which $25,000 can be requested from the sponsor with an additional $5,000 match from the respective College Dean. Special circumstances that warrant additional personnel may be addressed and larger budget amounts will be considered on rare occasions. Allowable budget categories include salaries and benefits for graduate students and post-doctoral students, supplies and expenses to support the research of these individuals including infrastructure and capital purchases for equipment necessary to launch, support and sustain the research activities.

The stipend for the principal investigator is limited to $7,500. Fringe benefits are not included for principal investigators with nine-month appointments but may be required for other salaries.

Budget changes exceeding 10% of the total award and re-budget of funds into categories not in the original budget (i.e. equipment, foreign travel, etc.) are subject to prior approval. Requests for re-budgeting must be made in writing to UD Cybersecurity Initiative (cybersecurity@win.udel.edu) and should include the reason for and details about the request and potential impact on the originally proposed project.

## PROJECT DURATION

UD CSI grants are awarded for up to two years, February 1 through January 31. The project period may be extended when circumstances warrant. Requests for no-cost extensions must be made in writing to the UD Cybersecurity Initiative (cybersecurity@win.udel.edu). Requests should include the reason for and the duration of the extension. A final report is due to the UD Cybersecurity Initiative (cybersecurity@win.udel.edu) no later than 90 days from the end date of the proposal.

## PROCEDURE FOR SUBMITTING PROPOSALS

All UD CSI grants require matching funds from the Principal Investigator's (PI) College. PIs must submit a full proposal, which cannot exceed two pages to request the matching funds. Information in excess of six pages will not be considered by the UD Cybersecurity Research Grant Committee. The Executive Summary, which should not exceed 250 words, is included as part of the six pages and should provide an overview of the scientific scope of the project and potential sources of future funding for the program. In addition to the six pages of the UD CSI proposal, a budget page (see Attachment 1) plus a budget justification are required.
**Reference citations may be included as an Appendix to the proposal*.

A two-page CV, following the NSF format for biographical information, is also requested. An NSF

example and template may be found on the UD CSI website at
http://csi.udel.edu/files/2015/09/UDCSI-NSF-Biosketch-Template-1djur9p.pdf
The full proposal must be created as a single file in Adobe PDF format. The proposal has to use one-inch margins and Times New Roman – 11 point font. It is important to avoid specialized terminology to aid the reviewers, who may have a variety of different technical specialties. Allow up to ½ page for Section 1 (Significance of the proposed work) and about 2 ½ pages for Section 2 (Description of proposed research or scholarly activity).

**A completed proposal and bio sketch should be emailed to** cybersecurity@win.udel.edu**.**

## DEADLINES

| | |
|---|---|
| UD CSI proposals due to UD Cybersecurity Initiative (udcsi@udel.edu) | **November 8, 2015** |
| Awards announced | January 8, 2016 |
| Funding available | February 1, 2016 |

## UNIVERSITY OF DELAWARE UNDERSTANDINGS CONCERNING UNIVERSITY OF DELAWARE CYBERSECURITY (UD CSI) GRANTS

UD CSI research grants are made with the following understandings. Acceptance of the award includes acceptance of these understandings.

1. The primary purpose of the research grant is to further the professional development of the recipient. In order to be selected for funding, the proposal must:

- ✓ Be an original contribution (20%)
- ✓ Be an important contribution (20%)
- ✓ Be something that a multidisciplinary team might be expected to complete in 1-2 years (20%)
- ✓ If successful, lead to significant, continuing funding by outside sources (e.g. NIH, NSF, DoE, DoD, USDA, State, Foundations, Private Sector, etc.) (30%)
- ✓ Have clarity of presentation (10%)

2. Research grants are awarded to early-career, untenured, tenure-track and tenured faculty members of the University. Acceptance signifies intent to continue at the University for the duration of the project period.

3. The University exercises no direction or supervision over the details of the research to be performed, but it does require adherence to the original objectives and purposes of the research. It also requires that a final report on the research be submitted to the UD Cybersecurity Initiative, no later than Ninety (90) days after the termination date of the grant. Each grantee is requested to furnish one copy of any resulting papers, books, or other publications to the UD Cybersecurity Initiative (cybersecurity@win.udel.edu).

4. Every publication directly resulting from a research grant must include an acknowledgment that the research was carried out with the support of the University of Delaware Cybersecurity Initiative.

5. Unless arrangements to the contrary have been included in the proposal as accepted, financial income derived from the project will be returned to the University, up to the amount of the award. This is not meant to conflict with University policies on patents, copyrights, and publications.

**Please see UD CSI Application here:**

UD CSI Application