IU BLOOMINGTON

EMERGING AREAS OF RESEARCH

Abstract Template -- Due June 30, 2017

Title of initiative to be proposed:

Enhancing Digital Supply Chain Assurance

Name of lead PI, with title, department/school:

Von Welch, Director, Center for Applied Cybersecurity Research, Pervasive Technology Institute, OVPIT
vwelch@iu.edu, 812-856-0363

Key team member names and departments/schools (up to 10 names):

Prof. Mark D. Janis, Robert A. Lucas Chair and Director of the Center for Intellectual Property, Research, Maurer School of Law; Prof. Michael Mattioli, Associate Professor, Maurer School of Law; Prof. Steve Myers, Associate Professor and Director of Secure Computing Programs, School of Informatics and Computing; Prof. Scott Shackelford, Chair, IUBloomington, Cybersecurity Program, Director, Ostrom Workshop Program on Cybersecurity and Internet Governance, Associate Professor, Kelley School of Business

Description of area to be proposed. What constitutes this area of research or creative activity as emerging? (Word limit=500)

The Internet and the IT infrastructure of every organization originates from supply chains that include a variety of sources: commercial, open source, domestic, and foreign. Even large agencies such as the U.S. Department of Defense no longer build their own IT infrastructure and instead rely on complex supply chains. Since IT systems control everything from phones to factories, ensuring these systems are secure is of vital importance to the global economy. Yet this is a daunting proposition given varying sources of insecurity, from malicious — a 2012 Microsoft report found malware being installed in PCs at factories in China — to conflicting commercial incentives, such as Lenovo's installation of advertising software that weaken security in 2015. Our overarching research question is how to enhance cybersecurity in the context of modern supply chains, a key challenge to both public and private sectors with a grand scope impacting a variety of IT systems, voting systems, vehicles, medical devices, and other "Internet of Things" applications. We will focus on a particular use case, with a particular medical device the leading contender. Research will address the development of technical countermeasures, analytics, and the crafting of appropriate incentive structures through empirical studies, technical innovation, and groundbreaking governance research. Current participants are the School of Informatics and Computing, the Kelley School of Business (including the Operations and Decision Technologies Department), the Maurer School of Law, the Center for Applied Cybersecurity Research (CACR), and the Ostrom Workshop.

Please submit to earprogram@indiana.edu