FOR IMMEDIATE RELEASE:

MDISS Launches 'WHISTL': an independent, non-profit network of security testing labs for medical devices.

MDISS WHISTL will focus on vetting complex multi-vendor, multi-device critical care environments like Hospital Intensive Care Units, Operating Theatres and Emergency Rooms

SAN FRANCISCO, CA - July 27, 2017 – MDISS, the Medical Device Innovation, Safety and Security Consortium today launched the first of more than a dozen planned device security testing labs and cyber-ranges. The new MDISS World Health Information Security Testing Lab (WHISTL) facilities will comprise a federated network of medical device security testing labs, independently owned and operated by MDISS-member organizations including healthcare delivery organizations, medical device manufacturers, universities and technology companies. Each WHISTL facility will launch and operate under a shared set of standard operating procedures. The goal is to help organizations work together to more effectively address the public health challenges arising from cybersecurity issues emergent in complex, multivendor networks of medical devices.

While such security 'proving grounds' aren't new to enterprise IT, WHISTL is the first network of labs specifically designed around the needs of medical device researchers, healthcare IT professionals and hospital clinical engineering leaders. By the end of 2017, MDISS WHISTL facilities will open in New York, Indiana, Tennessee, California as well as in the UK, Israel, Finland and Singapore.

Enabling MDISS members to test devices in both physical and virtual environments, WHISTL facilities will focus on identifying and mitigating medical device vulnerabilities, sharing solutions and best practices, and device security education and awareness. Newly uncovered vulnerabilities will be responsibly reported to medical device manufacturers and to the NHISAC-MDISS Medical Device Vulnerability Program for Evaluation and Response, or 'MDVIPER' at https://mdviper.org/

"WHISTL will provide much-needed insight from actual developers and users of medical devices, which will result in increased relevant and actionable information sharing and situational awareness for all stakeholders in healthcare”, said Denise Anderson, president of NH-ISAC, the National Health Information Sharing and Analysis Center. “NH-ISAC looks forward to partnering with MDISS on this important effort for the community.”

MDISS, established in 2010, is a 501(c)(3) non-profit organization operating as public-private partnership. Together with NH-ISAC, MDISS has already built a dynamic national cyber information-sharing community to advance patient safety and privacy. MDISS, under a $1.8M contract from the Department of Homeland Security (Science and Technology Directorate, Cyber Security Division) built the medical device cyber risk assessment platform, or ‘MDRAP’. The platform helps health systems, device manufacturers, and technology firms collaborate to produce and share device risk assessments. The fast-growing and standards-based MDRAP platform features moderated crowdsourcing and facilitates timely, responsible sharing of risk assessments and threat indicators, while helping automate critical device inventory, audit, oversight and vulnerability tracking tasks for hospitals.

Dr. Nordenberg, MD, Executive Director of MDISS, is a public health physician, medical epidemiologist and medical informatics expert. Formerly CIO at the National Centers for Disease Control’s National Center for Infectious Diseases, stated, “MDISS WHISTL facilities will dramatically improve access to device security know-how while protecting patient privacy and stakeholder intellectual property. Solid cyber-lab governance will support an international-scale network of research and training centers of excellence, designed especially for medical device designers, hospital IT, and clinical engineering professionals.” Nordenberg continued, “MDISS WHISTL testbeds will work also work closely with our partners at UL to advance best practices for security assessments based on emerging standards like UL 2900 and AAMI 80001.”

WHISTL’s device testing protocols will have their foundation in the UL Cybersecurity Assurance Program specifications (UL CAP), especially with regards to fuzz testing, static binary analysis and structured penetration testing. More information about UL CAP can be found here: http://industries.ul.com/cybersecurity “Being proactive in addressing interconnected medical device cybersecurity challenges is crucial to patient safety and risk management," states Anura Fernando, Principal Engineer Medical Systems Interoperability at UL. "We're pleased a growing number of emerging programs like WHISTL recognize and are utilizing UL 2900 to help address critical risks."

Benjamin G. Esslinger, CBET Manager/Clinical Engineer at Eskenazi Health, said "Working with MDISS over the past year on WHISTL has helped us make real progress against some very complex risk scenarios, while keeping the focus on patient safety." Esslinger is the current 2017 Trustee and past President of the Indiana Biomedical Society. He works with Matthew S. Dimino, an Imaging Engineer at Eskenazi Health and educator at Indiana University - Purdue University Indianapolis. Esslinger continued, "Remember, medical devices are still on the frontier of cybersecurity, and security best practices for devices are still maturing. Our new WHISTL facility enables us to run medical devices through tougher, more realistic test regimes. Hidden vulnerabilities surface more quickly, and that helps us build more responsive standard operating procedures."

Joshua Corman, a member of the U.S. Congressional Task Force on Healthcare Cybersecurity, founder of cyber safety initiative "I am The Cavalry" and the director of cyber statecraft for the Atlantic Council think tank said, "Ambitious initiatives like WHISTL are sorely needed, and I look forward to supporting MDISS in this undertaking. Through our over-dependence on undependable things, we have created conditions where accidents and adversaries can have a profound impact on public safety and human life. Undirected attacks like 'WannaCry' were sufficient to impact patient care at 65 hospitals in the UK. A known vulnerability in a single device recently shut down care at Hollywood Presbyterian Hospital. Hospitals are prone, they are prey. Now the predators have taken notice."

Billy Rios, CEO at Whitescope, a deep security research and advisory firm, said "Patient encounters with connected yet poorly secured medical devices are increasing exponentially, and nobody really has a handle on the risks we're facing. We've got to integrate best practices from cybersecurity, public health and clinical engineering disciplines to better understand and mitigate these threats, and the new MDISS network of WHISTL device testing and data sharing facilities are a huge step in the right direction."

Mike Ahmadi, Global Director for Critical Systems Security at Synopsys, said "I am very happy to see organizations like MDISS taking the bold initiative to build and maintain test environments for the healthcare space. Test labs where devices and systems can be assessed for vulnerabilities and proper deployment are the only way we can reach some level of cyber assurance. I applaud these efforts."

MDISS WHISTL is part of a comprehensive public health initiative: The National Health Cyber Safety Network for Technology. This initiative aims to develop best practices to advance public health and patient safety by expanding access to evidence-based security data and hardening health care infrastructure against cyberattacks. MDISS partners closely with the National Healthcare Information Sharing and Analysis Center (NH-ISAC), to facilitate the timely sharing of medical device vulnerabilities, threat indicators and mitigation measures in the healthcare community. MDISS and NHISAC are working together to foster cooperation on health-tech best practices, education and policy initiatives to proactively mitigate risks associated with the proliferation of connected medical devices.

For more information about WHISTL, contact MDISS at whistl@mdiss.org

ABOUT MDISS – The Medical Device Innovation, Safety and Security Consortium (MDISS), founded in 2010, is a 501(c)(3) non-profit public/private partnership dedicated to advancing patient safety and public health, and the first to focus exclusively on medical device cybersecurity. MDISS develops and delivers practical technology, operations and policy solutions for member organizations, including hospitals, health delivery organizations, doctors, epidemiologists, clinical engineers, medical device manufacturers, academics, regulators, embedded security experts and cybersecurity researchers. Join us. Visit www.mdiss.org.

ABOUT NH-ISAC – The National Health Information Sharing and Analysis Center (NH-ISAC), the official healthcare information sharing and analysis center, offers non-profit and for-profit healthcare stakeholders, such as: independent hospitals, IDN providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical school and medical R&D organizations, a community and forum for sharing cyber and physical threat indicators, best practices and mitigation strategies. NH-ISAC is a non-profit corporation funded and owned by its members. Visit www.nhisac.org.

Media Contact:
Kurt Stammberger, CISSP PMC
+1-415-519-0840
kurt.stammberger@mdiss.org

###