March 14, 2019

Dear Members of the U.S. Congress,

We the undersigned organization write in support of the vital role that WHOIS domain name registration data plays in cyber security and cyber investigations. While the value of WHOIS data is widely known throughout the cyber security industry, its day-to-day use is less known elsewhere. We are gravely concerned that recent policy changes have effectively blocked access to this critical data set.

As you may know, WHOIS data is the publicly available information on *who* has registered a particular internet domain name. In layman's terms, WHOIS records are akin to land title or property tax records: a record of who owns the internet property of domain names available in .com, .net, and other generic top-level domain (gTLD) name spaces. Each WHOIS record contains basic contact information for the domain name registrant: name, address, phone number and email address, and certain other technical attributes. Since the dawn of the internet as we know it, gTLD registrars and registries – those companies who sell domain names – have collected contact information from all registrants at the time of registration.

WHOIS data is critical to law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, intellectual property rightsholders, journalists, academics and others. These stakeholders all rely on WHOIS to help them determine *who is* operating a criminal website, sending malicious (spam, phishing) emails, conducting cyber-attacks, influencing elections, propagating fake news or committing fraud under the guise of a known brand. In these instances, WHOIS data is used to identify and collect lists of domain names that investigators associate with a given criminal or cyber-attack and to identify the likely perpetrators of these attacks. In criminal investigations, for example, listing domains and making connections using contact information is imperative to understanding and interdicting criminal, terrorist, or hostile nation state activity to its fullest extent.

Because of an overly broad interpretation of the EU's General Data Protection Regulation (GDPR), many domain name registrars and registries are shutting down public access to WHOIS data. This has the effect of impeding our cyber investigations, limiting our ability to protect American consumers and businesses, and destabilizing the security of the open web. Already, cyber investigators and counter-terrorist agents are experiencing difficulties in utilizing the WHOIS database to the degree it was available prior to the interpretation of the EU GDPR and we expect this issue to continue to worsen.

We encourage the U.S. Congress to educate itself on the critical function that WHOIS data plays in protecting its citizens from fraudulent or otherwise criminal behavior and ask you to take steps to ensure public access to this essential tool.

Signed,

Robert Olsen, Global Practice Leader - Cybersecurity, Senior Managing Director, Ankura Consulting

Dave Jevans, Chairman of the Board of Directors, Anti-phishing Working Group

Peter Cassidy, Secretary General, Anti-Phishing Working Group

Gretchen Peters, Executive Director, Center on Illicit Network and Organized Crime

Lisa A Phifer, President, Core Competence

Bret Padres, Chief Executive Officer, The Crypsis Group

Alison Nixon, Director of Security Research, Cybersecurity Investigator

Tim Chen, CEO, DomainTools

Anthony J. Ferrante, Head of Cybersecurity & Senior Managing Director, Global Risk & Investigations Practice, FTI Consulting

Caleb Barlow, VP, X-Force Threat Intelligence, IBM Security

David Piscitello, Principal, Interisle Consulting Group

Susan Estrada, founder CERFnet, Internet Hall of Fame

Jeffrey Bedser, CEO/President (on behalf of), iThreat Cyber Group

Winston Krone, Global Managing Director, Kivu Consulting

Alan Brill, Senior Managing Director – Cyber Risk, Kroll, a division of Duff & Phelps

Jason N. Smolanoff, Senior Managing Director, Global Practice Leader - Cyber Risk, Kroll, a division of Duff & Phelps

John Horton, President & CEO, LegitScript

Carmen Catizone, Executive Director, National Association of Boards of Pharmacy

Matt LaVigna, CEO, National Cyber-Forensics and Training Alliance

Stewart Baker, Former General Counsel of the National Security Agency, Former Assistant Secretary for Policy at the Department of Homeland Security

Shabbir Safdar, Executive Director, Partnership for Safe Medicines

Thomas Kubic, President & CEO, Pharmaceutical Security Institute

Jeremiah Dewey, Senior Director, Rapid7

Kiran Belur, Head of Trademarks and Copyrights, Salesforce

Saeed Abu-Nimeh, CEO, Seclytics

Norm Ritchie, Chair, Secure Domain Foundation

Heidi Garfield, General Counsel, Shutterstock

Chris Loehr, President, Solis Security

Eric Friedberg, Co-President, Edward Stroz, Co-President, Stroz Friedberg, an Aon company

Serge D. Jorgensen, Founding Partner and Chief Technology Officer, Sylint Group

Libby Baney, Senior Advisor, Alliance for Safe Online Pharmacies

Joe St. Sauver, Ph.D., Security Professional