FOR IMMEDIATE RELEASE

Kroll Names Stacy Scott Managing Director in Cyber Security and Investigations Practice, Dallas

Information Security Professional with Expertise in Cyber Risk Management, Security Program Development, and Healthcare Regulatory Compliance

NEW YORK – October 2, 2017 – Kroll ("the Company"), a global leader in risk mitigation, investigations, compliance, cyber resilience, security, and incident response solutions, today announced the appointment of Stacy Scott as a Managing Director in its Cyber Security and Investigations practice, based in Dallas. In addition to founding and operating her own consultancy, Scott has served in high-profile roles with a leading cyber security consulting firm, a Big Four accounting firm, and the largest not-for-profit healthcare system in Texas. Over the past 16 years, she has built a successful track record of developing and implementing strategic information security initiatives that help organizations better safeguard data, manage risk, and enhance business operations.

"Stacy brings a wealth of information risk management experience, with particular expertise in cyber risk management, security program development, and regulatory compliance, especially in the healthcare sector," said Jason Smolanoff, Senior Managing Director and Global Cyber Security Practice Leader for Kroll. "With her advanced technical knowledge in multiple facets of information security, broad leadership experience, and ability to forge productive relationships within organizations, from boards of directors to front-line staff, Stacy will enhance our ability to deliver outstanding results to our clients across the globe."

"On behalf of our clients and our company, I am delighted to welcome Stacy to our Cyber Security team," said David Fontaine, Chief Executive Officer of Kroll and its parent, Corporate Risk Holdings. "Stacy is a dynamic professional who excels at helping enterprises transform information security into a competitive advantage. I am confident our clients will quickly recognize in Stacy a valued advisor who brings to each engagement a unique combination of technical expertise, business acumen, and strategic vision."

Most recently, Scott was the President and Founder of Wisterwood Advisory Services. From 2014-2016, Scott served as Vice President, Security Science for Stroz Friedberg in Dallas. Scott was the firm's HIPAA Security Rule subject matter expert. From 2006-2014, Scott was Director, Enterprise Architecture and Security, for Baylor Scott & White Health, the largest not-for-profit healthcare system in Texas, with over 34,000 employees, 5,400 licensed beds, and 43 locations. In this role, which was the healthcare system's highest-ranking information security position, Scott directed and oversaw the development and implementation of the enterprise's overall information security architecture as well as security strategy and programs, managing a multimillion-dollar budget. Scott's accomplishments included developing and executing the plan to overhaul security tools in order to mature monitoring processes and rules to enable rapid detection and response to potential security incidents. These efforts reduced the risk of compromise to enterprise systems, including the possible loss of financial data and personal health information.

During this time, Scott also served as the healthcare system's HIPAA Security Officer. She possesses a deep understanding of financial and healthcare regulations, including NIST Policy, Federal Trade Commission Red Flag Rules, HIPAA Security Rules, PCI (Payment Card Industry) Data Security

Standards, and the American Recovery and Reinvestment Act (ARRA) Health Breach Notification Rule. Scott also chaired the system's information security council that worked to assist business users in making the appropriate security risk decisions consistent with the organization's goals and risk levels. Earlier in her career with Baylor Scott & White, Scott was Director, Standards, Audit, & Integration; Manager, Internal IT Audit; and Information Security (IS) Security Engineer. Scott began her professional career as a Senior Information Risk Management Consultant for KPMG, where she conducted assessments of information system security access, change and lifecycle development management, and computer operations for major ERP systems, such as SAP, Oracle, JD Edwards, and PeopleSoft.

Scott earned her Bachelor of Business Administration degree in Information & Operations Management at Texas A&M University. In addition to holding certifications as an Information Systems Auditor and HITRUST Common Security Framework Practitioner, Scott is a member of CHIME (College of Healthcare Information Management Executives); HIMSS (Healthcare Information Management Systems Society); ISACA (Information System Audit & Control Association); and AITP (Association of Information Technology Professionals). In testament to her extraordinary record of achievement, Scott was recognized as Woman of the Year by the National Association of Professional Women in 2012.

About Kroll:
Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. Headquartered in New York with more than 35 offices in 20 countries, Kroll has a multidisciplinary team of nearly 1,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies and individuals. For more information visit www.kroll.com.

Forward-Looking Statements
This press release may contain "forward-looking statements." These forward-looking statements include, but are not limited to, statements regarding the Company's performance and growth, and other non-historical statements. Forward-looking statements identify prospective information. Important factors could cause actual results to differ, possibly materially, from those stated in the forward-looking statements. In some cases you can identify forward-looking statements by words such as "anticipate," "believe," "could," "estimate," "expect," "intend," "may," "plan," "predict," "potential," "should," "will" and "would" or the negatives thereof, variations thereof or other similar words. You should read statements that contain these words carefully because they discuss the Company's future priorities, goals, strategies, actions to improve business performance, market growth assumptions and expectations, future business opportunities, capital expenditures, financing needs, financial position and other information that is not historical information or state other "forward-looking" information. Forward-looking statements should not be read as a guarantee of future performance or results, and will not necessarily be accurate indications of the times at, or by which, such performance or results will be achieved. Forward-looking information is based on information available at the time and/or management's good faith belief with respect to future events, and is subject to risks and uncertainties that could cause actual performance or results to differ materially from those expressed in the statements. Forward-looking statements speak only as of the date the statements are made. The Company assumes no obligation to update forward-looking statements to reflect actual results, changes in assumptions or changes in other factors affecting forward-looking information except to the extent required by applicable securities laws. If the Company does

update one or more forward-looking statements, no inference should be drawn that the Company will make additional updates with respect thereto or with respect to other forward-looking statements.

Contacts:
Kroll (U.S. Contact)
Nicole Cueto
212-833-3481
Nicole.Cueto@kroll.com

Media Contact:
Infinite Global
Ada Oni-Eseleh
646-685-8075
AdaOE@infiniteglobal.com