BAI Information Security Introduces *"Risk Management Framework (RMF) for DoD IT"* Training Program

Addresses Transition from DIACAP to New DoD Risk Management Methodology

Fairlawn, VA - (March 31, 2014) – BAI Information Security today announced the latest update to its cybersecurity risk management training portfolio. The *Risk Management Framework (RMF) for DoD IT* training program covers the newly-unveiled DoD risk management methodology and the process of transition from the legacy DIACAP process. With the release of DoD Instructions 8500.01 and 8510.01 earlier this month, the Department of Defense has entered into a long awaited "transformation" that will ultimately bring its IT risk management practices into harmony with those of the federal civil agencies and intelligence community, forming a "unified framework for information security and risk management" across the government. The new process has been dubbed "RMF for DoD IT", and relies heavily on guidance published by the National Institute for Standards and Technology (NIST) and the Committee on National Security Systems (CNSS).

"These DoD publications are the culmination of a long, grueling planning process that has taken place within the Pentagon's walls," said Lon Berman, Principal Consultant and Training Director of BAI. "The DoD IT community has been anxiously awaiting this announcement for quite some time, and the need for training in the new process is well understood."

To that end, BAI is offering a four-day training program beginning in April, 2014, consisting of a one-day ***RMF for DoD IT – Fundamentals*** class, followed by a three-day ***RMF for DoD IT – In Depth*** class. The training program includes coverage of the basic tenets of cybersecurity and risk management and the extensive legislative and policy background underlying RMF. The bulk of the class time is spent on RMF roles and responsibilities, life cycle process steps, documentation requirements, security controls (requirements), and the all-important transition process from DIACAP to RMF.

"As with all our training programs, we present an optimal mixture of government policies/guidance and practical knowledge," Berman explained. "We want our students to go back to their workplaces with a good understanding of what DoD expects of them and some practical skills to help them get it done."

The *RMF for DoD IT* training program is open to DoD employees as well as supporting contractors, service providers, and suppliers. Anyone who needs a better understanding of the new DoD cybersecurity landscape will benefit from this training.

BAI is offering *RMF for DoD IT* training on a regularly-scheduled basis at several training centers, as well as through its Personal Classroom™ methodology (online, instructor-led sessions). Classes are open for registration at http://register.rmf.org. Additionally, organizations with a group of potential students can arrange for on-site training at their own facility.

About BAI Information Security

BAI Information Security is a trusted provider of training and consulting services to the Department of Defense and other federal agencies, along with their supporting contractors and vendors. BAI's service methodology is based on the Risk Management Framework (RMF) developed by the National Institute of Standards and Technology (NIST) in partnership with the Joint Task Force Transformation Initiative (JTFTI). To date, BAI has trained thousands of students internationally on DIACAP, RMF, FISMA and Continuous Monitoring, and has provided consulting services to numerous government agencies and Fortune 500 companies. BAI is headquartered in Fairlawn, VA. For more information, please visit: www.rmf.org, or contact Annette Leonard, Director of Marketing, 1-800-RMF-1903 X104.