Media Contact:
Stacy Simpson
Policy and Communications Director
SAFECode
703-812-9199
stacy@safecode.org

FOR IMMEDIATE RELEASE

SAFECode Releases Framework for Software Supply Chain Integrity

New Paper Defines Risks and Responsibilities for Securing Software in the Global Supply Chain

Arlington, Va. – July 21, 2009 – The Software Assurance Forum for Excellence in Code (SAFECode), a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods, today released "*The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain."* The paper outlines the first industry-driven framework for analyzing and describing the efforts of software suppliers to mitigate the potential that software could be intentionally compromised during its sourcing, development or distribution. The paper was jointly developed by SAFECode's members, which include EMC Corporation, Juniper Networks, Inc., Microsoft Corp., Nokia, SAP AG and Symantec Corp.

As the software industry has become increasingly globalized, a concern has risen over the possibility that an IT solution could be compromised by the intentional insertion of malicious code into the solution's software during its development or maintenance, which is often referred to as a supply chain attack. Though experts have concluded that the supply chain is not the most likely attack vector, vendors are taking action to mitigate supply chain risk by applying software integrity practices - the collection of processes and controls that enable a vendor to deliver customers a product that is uncompromised, thereby containing only what the vendor intends.

"While SAFECode's members have individually implemented software integrity practices, this is the first time industry has come together to establish a common framework for ensuring the integrity of software through the global supply chain," said Paul Kurtz, executive director of SAFECode. "This framework will serve as the foundation for subsequent work aimed at identifying and analyzing software integrity best practices and represents a critical step forward in the industry's efforts to advance software assurance."

Software assurance is most frequently discussed in the context of ensuring that code itself is more secure through the application of secure software development practices. However, while there has been a growing and appropriate focus on eliminating software vulnerabilities through secure development practices, this represents only one element of software assurance. The processes for sourcing, creating and delivering software must also contain integrity controls to enhance confidence that the software functions as the supplier intended.

Within SAFECode's software supply chain integrity framework, software supply chain integrity controls address the access, storage and handling of development assets throughout the key links in the software supply chain – supplier sourcing, product development and testing, and product delivery. The controls are designed to be independent of geography, accommodate diverse sources of software components, and

extend from a vendor's suppliers to its customers. Software supply chain integrity practices and controls derive from established security and integrity principles, including:

- **Chain of Custody:** The confidence that each change and handoff made during the source code's lifetime is authorized, transparent and verifiable.
- **Least Privilege Access:** Personnel can access critical data with only the privileges needed to do their jobs.
- **Separation of Duties:** Personnel cannot unilaterally change data, nor unilaterally control the development process.
- **Tamper Resistance and Evidence:** Attempts to tamper are obstructed, and when they occur they are evident and reversible.
- **Persistent Protection:** Critical data is protected in ways that remain effective even if removed from the development location.
- **Compliance Management:** The success of the protections can be continually and independently confirmed.
- **Code Testing and Verification:** Methods for code inspection are applied and suspicious code is detected.

SAFECode will build upon this framework for software supply chain integrity with a focused effort to identify and analyze the most effective software integrity controls and practices that its member companies use to help ensure the integrity of their software. It will publish its findings later this year to help extend these practices across the industry and provide customers with additional insight into how to view and evaluate the processes by which software integrity is achieved.

"The complexities and interdependencies of the IT ecosystem require software suppliers to not only be able to demonstrate the security of products they produce, but also evaluate the integrity of products they acquire and use. For this reason, every software supplier has a significant stake in the identification, communication and evaluation of best practices for ensuring software integrity," said Kurtz. "By promoting the adoption of well-defined software integrity practices across the industry, these efforts should ultimately lead to increased customer confidence in the security of IT solutions."

A full copy of "*The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain"* is available for free download at http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf

About SAFECode
The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. SAFECode is a global, industry-led effort to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services. Its members include EMC Corporation, Juniper Networks, Inc., Microsoft Corp., Nokia, SAP AG and Symantec Corp. For more information, please visit www.safecode.org.

###