Supply Chain Vulnerabilities (U)

(U) Networks are not the only vulnerable aspect of cyberspace. Software and hardware are also at risk of being tampered with before they are linked together in an operational system. The majority of information technology products used in the United States are manufactured and assembled overseas. The reliance of DoD, and the United States as a whole, on foreign manufacturing and development provides broad opportunities for foreign actors to subvert and interdict U.S. supply chains at points of design, manufacture, service, distribution, and disposal. Additionally, counterfeit hardware and software have already been detected in systems that DoD has procured. Rogue code, including so-called "logic bombs" that can cause sudden malfunctions, can be inserted into software as it is being developed. Remotely operated "kill switches" and hidden "backdoors" can be written into the computer chips used by DoD or in critical infrastructure, allowing outside actors to manipulate the systems from afar. Tampering is difficult to detect and even harder to eradicate.

Supply Chain Risk Mitigation Framework (U)

(U) DoD will continue to support the development of whole-of-government approaches for managing the risks associated with the globalization of the information and communications technology sector. Many U.S. technology firms outsource software and hardware factors of production, and in some cases their knowledge base, to firms overseas; this presents adversaries with significant opportunities to interdict and subvert DoD systems. Additionally, increases in the number of counterfeit products and components demand procedures to both reduce risk and increase quality. Dependence on technology from foreign sources dimishes the predictability and assurance that DoD requires. The global technology supply chain affects mission critical aspects of the DoD enterprise, along with core U.S. government and private sector functions, and its risks must be mitigated through strategic public-private sector cooperation.

(U) In accordance with *Defense Programming and Planning Guidance for FY2012-2016* and specific DoD guidance, DoD is implementing a supply chain risk mitigation (SCRM) strategy with pilot activities and building toward full operational capability by FY16. DoD will continually implement and refine policies and processes that empower program managers, systems managers, and acquisition professionals to mitigate supply chain risk wherever they acquire, integrate, and maintain mission critical networks and systems.

(U) DoD also co-leads the SCRM initiative within the *Comprehensive National Cybersecurity Initiative* (CNCI). In this role, DoD is working closely with its interagency partners to implement a comprehensive SCRM strategy for other U.S. government national security systems. This collaborative effort will build upon lessons learned from efforts in DoD and across the government to address shared supply chain challenges.

(S//REL USA, FVEY) Supply chain risks also extend to U.S. critical infrastructure upon which DoD depends. An example of these risks can be found in the telecommunications sector, as Chinese telecommunications equipment providers (non-public companies with suspected ties to the People's Liberation Army) pursue inroads into the U.S. telecommunications infrastructure. DoD is working with its interagency partners to develop and implement a multifaceted approach to SCRM that supports vital government operations and provides a high degree of information security in a potentially unsecure infrastructure.

(S//REL USA, FVEY) In conjunction with departments and agencies addressing trade and economic security, the SCRM strategy will promote a diverse and competitive global marketplace for trusted technology. The objectives of this initiative are to: 1) manage and mitigate the risk of untrustworthy technology used by the telecommunications sector; 2) promote an open the global marketplace and a level commercial playing field for technology used by the telecommunications sector; 3) enhance the viability of U.S. science, technology, and advanced manufacturing capabilities to achieve and support national security objectives. This plan is being developed with a whole-of-government approach, in cooperation with industry as appropriate, to ensure U.S. ability to project force, complete intelligence missions, and protect the functioning of the national economy