FOUO

INFORMATION PAPER

August 15, 2008

SUBJECT: U.S. Army's Concerns with Protection of Controlled Unclassified Information

1. Purpose. To inform the Under Secretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L)) of the U.S. Army's concerns with protection of controlled unclassified information (CUI) under the control of Defense Industrial Base (DIB) contractors and actions to address these concerns.

2. Issues:

a. Defense acquisition regulations, directives, and guidance address aspects of risk management but have not kept pace with the risks posed by two major trends that impact the DIB at least as much as other sectors of the economy: (1) Digitalization of information and (2) globalization of economic activity.

(1) Digitalization of information has introduced greater risk of compromise of DIB-held Department of Defense (DoD) controlled unclassified program information that is used in the development of Warfighting systems during the acquisition life cycle. Simply stated, hostile actors can exfiltrate large volumes of unclassified program information in a single attack that can potentially net enough information to enable adversaries to narrow a capability gap. Exfiltrations of unclassified data from DIB unclassified systems have occurred and continue to occur, potentially undermining and even neutralizing the technological advantage and combat effectiveness of the future force.

(2) Globalization of economic activity has expanded the DIB to include more non-U.S. companies and increased DoD's reliance on suppliers from outside the United States. An increase in foreign suppliers, especially of key information technology components, raises the risk that adversaries could insert malicious or counterfeit components into U.S. Army weapons systems.

b. These trends necessitate a much more comprehensive approach to acquisition risk management than has traditionally been the case. Current program protection efforts largely focus on mitigating risks of compromise to Warfighting technologies as a result of traditional espionage or industrial theft but not on those associated with broader risks posed by these trends. The recently published DoD Instruction 5200.39, Critical Program Information (CPI) Protection within the Department of Defense, will

help address these trends by updating and clarifying definitions, responsibilities and roles for protecting critical program information.

3. U.S. Army Approaches:

a. U.S. Army Defense Industrial Base Cyber Security Task Force (DIB CSTF). Because no single office of primary responsibility existed within the U.S. Army to manage these and other emerging risks, the Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)) created the DIB CSTF, which is responsible for organizing and coordinating U.S. Army efforts to mitigate risk to U.S. Army acquisition programs. The DIB CSTF is primarily focused on countering the potentially detrimental impact associated with cyber exfiltration of CUI from DIB unclassified networks.

b. Policy Development. The Army DIB CSTF is leading, in coordination with components of the Office of the Secretary of Defense, a Tri-Service Cyber Security Acquisition initiative that is intended to provide DoD an empirical basis—including viable contract language, budgetary impacts and Defense Federal Acquisition Regulations/Federal Acquisition Regulation revisions—to evaluate potential permanent solutions for protecting CUI on DIB networks.

c. Damage Assessment. The Army DIB CSTF is coordinating an interagency pilot program to assess information compromised through computer intrusions against DIB contractor systems to determine whether there may have been compromises of data on current and future U.S. Army weapons program, scientific and research projects and warfighting capabilities that could cause a loss of technological advantage against our adversaries. The Army process will serve as DoD's model for acquisition program damage assessments.

d. Supply Chain Risk. The Army DIB CSTF is working with OSD offices, including the Office of the Under Secretary of Defense (Acquisition, Technology and Logistics), Office of the Assistant Secretary of Defense (Networks and Information Integration) and others to develop policy to manage the risk that adversaries might insert corrupted or malicious technology into components—some of which may come from outside the United States DIB—that are bound for DoD critical systems to later gain unauthorized access to data, alter data or sabotage communications. The focus of the Army effort will be on companies in the command, control, communications, intelligence, surveillance and reconnaissance categories, or technologies that affect U.S. Army modernization efforts or security of research, development, test and evaluation facilities, program offices and/or supply chains.

4. Future Actions:

a. Critical Program Information Protection. U.S. Army DIB CSTF will work across the Army to integrate the requirements identified in the newly published DoD Instruction 5200.39 through interface with the Headquarters, Department of the Army elements, Program Executive Offices and their respective Project/Product Managers and U.S. Army Materiel Command to ensure synchronization of Army priorities and requirements established under the Research, Technology Protection, and Critical Infrastructure Protection programs.

b. Horizontal Protection. Technologies similar to those used by the U.S. Army are found in other military service research and development programs and weapons systems. The Army DIB CSTF will coordinate with USD(AT&L) and the other military service acquisition authorities to ensure like technologies are afforded the same level of protection.

c. Risk Management. Transition the Army DIB CSTF to a fully funded permanent office within ASA(ALT) to integrate risk management into all facets of the research, development, test and evaluation and acquisition process and lifecycle management, including DIB cybersecurity efforts.

5. Budget. Funding to support operation of the U.S. Army DIB CSTF accounts for personnel, travel, and equipment and supplies and is depicted for the period Fiscal Years 2010-2015. Funding will need to be secured in order to permanently establish an office designed to oversee program protection and risk management planning with the U.S. Army.

	POM 10-15						
MDEP XMGH	FY 10	FY11	FY12	FY13	FY14	FY15	TOTAL
Salary	$1,165,517	$1,165,517	$1,165,517	$1,165,517	$1,165,517	$1,165,517	$6,993,102
Travel	$16,500	$16,500	$16,500	$16,500	$16,500	$16,500	$99,000
Supplies	$17,440	$17,440	$17,440	$17,440	$17,440	$17,440	$104,640
TOTAL	$1,199,457	$1,199,457	$1,199,457	$1,199,457	$1,199,457	$1,199,457	$7,196,742

Ray Gagne/693-6794
Approved By: Mr. Velz