



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

OCT 31 2012

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Defense Industrial Base Cyber Security

Cyber security is critical to all Department of Defense (DoD) missions, which increasingly rely on our private sector partnerships with the Defense Industrial Base (DIB). Cyber threats to DIB unclassified information systems represent an unacceptable risk of compromising DoD information and pose an imminent threat to U.S. national security and economic security interests. As a key element of the Department's multi-pronged approach to DIB cyber security, all DoD Components should actively encourage their eligible, cleared contractors to consider participating in the voluntary DIB Cyber Security and Information Assurance (CS/IA) program and its optional DIB Enhanced Cyber Security Services (DECS) component.

The DoD's DIB CS/IA program enhances and supplements DIB participants' capabilities to safeguard DoD information that resides on or transits DIB unclassified information systems. Current DIB CS/IA participants attest to the material benefits and value of the program in improving their network security posture, architectures, and capabilities to protect DoD information.

Under the DIB CS/IA program, DoD provides classified and unclassified cyber threat information and information assurance best practices to DIB companies. DIB participants, in turn, report cyber incidents that may involve DoD information for analysis, development of coordinated mitigation strategies, and, when needed, cyber intrusion damage assessments of compromised DoD information.

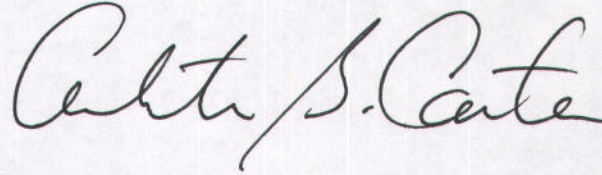
Through the optional DECS component of the program, the U.S. Government furnishes classified cyber threat and technical information, either to a DIB company or to the DIB company's authorized DECS Commercial Service Provider, to counter additional types of known malicious cyber activity.

The DIB CS/IA program, with its associated DECS component, enables unprecedented cyber security collaboration between DoD and the private sector. Although threats cannot be eliminated, this voluntary partnership between DoD and the DIB strengthens our collective protection against this real, immediate, persistent, and increasingly sophisticated cyber threat. Similarly, the program's success is keenly dependent on fostering a trusted information sharing environment, in which all participants are dedicated to preserving the security and integrity of the sensitive information being shared, and to ensuring the protection of individual privacy and civil liberties.



OSD012537-12

DoD Components should inform their eligible industry partners that they may apply to the DIB CS/IA program and find additional information at the publicly accessible website <http://dibnet.dod.mil>. Questions regarding the DIB CS/IA program can be directed to Ms. Victoria Morgan, Director, DIB CS/IA Program at email: Victoria.Morgan@osd.mil, 1-855-363-4227.



DISTRIBUTION:
SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMAND
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES