

YOU NEED TO KNOW

Protecting weapon systems program information: A policy and legislative update

by Peter M. Velz

DOD policy on cyber security and program protection is undergoing significant changes, in recognition of the increased threat to the integrity of weapon, communications, and information systems resulting from the reliance of these systems on digitized information and the possible compromise of program information used to develop and build those systems.

NETWORK SECURITY

The integrity of weapon systems increasingly depends on managing the risk of losing the most sensitive unclassified program information to cyber attacks on contractors' unclassified networks by our adversaries. (Army AL&T Magazine file photo image.)

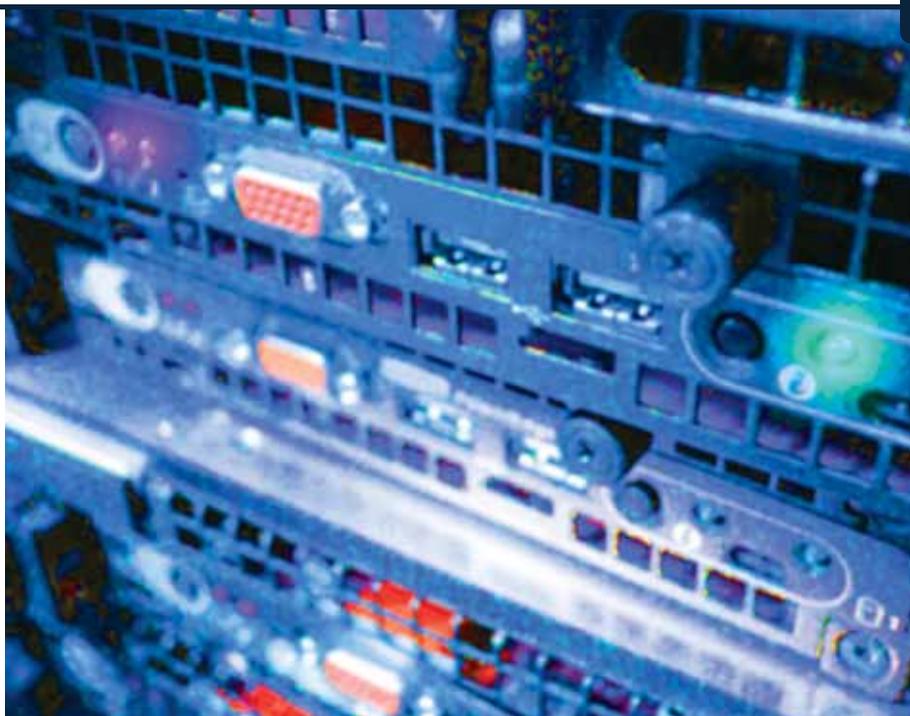
To address these complex challenges and enhance the likelihood that acquisition program managers (PMs) can deliver systems to the warfighter that function as intended, DOD is conducting pilot programs to develop new risk mitigation strategies, concepts, and processes.

Congressional interest in and support for these efforts gained significant traction in the *National Defense Authorization Act (NDAA) for Fiscal Year 2011*. Within the Army, the Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASAALT) is coordinating these policy efforts as they mature. They increasingly will become a standard part of acquisition program risk management, taking into account a variety of factors, such as cost, threat, criticality of particular components to a system's functionality, and technological lead relative to potential adversaries.

POLICY UNDERPINNINGS

It is DOD policy that the Department, its contractors, and its subcontractors will provide adequate security to safeguard DOD information on their unclassified information systems from unauthorized access and disclosure. The integrity of weapon systems increasingly depends on managing the risk of losing the most sensitive unclassified program information to cyber attacks on contractors' unclassified networks by our adversaries. DOD Instruction (DODI) 5205.13, *Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities*, dated Jan. 29, 2010, establishes the policy framework for DOD's main effort to work with DIB partners within a pilot program to mitigate that risk.

This instruction directs the heads of DOD components to, among other things, "Based on USD(AT&L) [Undersecretary



DOD NETWORK

Mission-critical functionality of DOD's systems and networks extensively leverages commercial, globally interconnected, globally sourced information and communications technologies. (U.S. Army photo.)

of Defense for Acquisition, Technology, and Logistics] policy guidance, develop procedures and conduct cyber intrusion damage assessments in support of DIB CS/IA activities to determine the overall impact of the exfiltration or modification of data on current and future weapons programs, scientific and research projects, and warfighting capabilities stemming from unauthorized intrusions into DIB unclassified information systems."

More specific policy directing the inclusion of language in contracts and agreements requiring protection of DOD information held by contractors is found in Directive-Type Memorandum (DTM) 08-027, *Security of Unclassified DoD Information on Non-DoD Information Systems*. Some examples of information assurance practices that should be addressed in contracts include:

- Do not process DOD information on public computers or on computers that do not have access controls.

- Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
- Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices or removable storage media, using the best available encryption technology.
- Limit information transfer to these subcontractors or teaming partners who have a need to know and a commitment to at least the same level of protection.

There is a recognition that further DOD guidance is needed to ensure that PMs and contracting officers have the tools they need to understand and implement this policy, including specific contract clauses, compliance assessment, and what is chargeable by the contractor.

Some of these issues are being addressed in the development of Defense Federal

Acquisition Regulation Supplement Case 2008-D028, *Safeguarding Unclassified Information*. This case would add a new subpart and associated contract clauses for the safeguarding, proper handling, and cyber intrusion reporting of unclassified DOD information that resides on or transits contractors' unclassified information systems.

DOD published notice of this case in the *Federal Register* on March 3, 2010, and held an initial public hearing on it on April 22, 2010.

Categories of DOD information that would require protection include: critical program information (CPI); information subject to export control under *International Traffic in Arms Regulations* and Export Administration regulations; personally identifiable information; and other categories of CUI.

Among other things, contractors would be required to:

- Implement information security in any project, enterprise, or company-wide unclassified information technology system using specified minimum security controls.
- Report to DOD any relevant cyber intrusion events.
- Support the forensic analysis of those data for purposes of conducting assessments of damage to acquisition and other programs.
- Procure and use only DOD-approved identity authentication credentials to, for example, receive emails from Army PMs containing data files with CPI.
- Include the substance of this clause in certain subcontracts.

TRUSTED DEFENSE SYSTEMS

Another key policy focus for mitigating risk of losing critical unclassified information is the effort to ensure trusted

defense systems by managing the supply chain risk for those systems, particularly to protect mission-critical software and hardware components. Mission-critical functionality of DOD's systems and networks extensively leverages commercial, globally interconnected, globally sourced information and communications technologies. Consequently, adversaries have more opportunities to corrupt technologies, introduce malicious code into the supply chain, and otherwise gain access to the Department's military systems and networks.

The policy framework to address this challenge is established by DTM 09-016, *Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems*. During development of a system, the PM determines which software and hardware components within the system are critical and then determines, based on identified threat and vulnerability, how to protect it with the support of

experts from various disciplines, including counterintelligence, intelligence, security, systems engineering, and policy.

This policy establishes a process that involves extensive collaboration among the DOD components to manage these risks. Army program executive officers (PEOs) and PMs engage in this process as part of the development and updating of their program protection plans at each milestone review.

KEY LEGISLATION

The congressional defense committees are playing a critical role in identifying and highlighting the need to improve cyber security. Two particular provisions in the NDAA for FY11 pertain to acquisition and address the issues outlined above. They are:

- Section 806, *Requirements for Information Relating to Supply Chain Risk*. Congress has given DOD new authority

COMPUTER DEFENSE ACTION

DODI 5205.13 establishes the policy framework for DOD's main effort to work with DIB partners within a pilot program to mitigate the risk of losing sensitive unclassified program information to cyber attacks. Here, Jerod Young, an analyst in a Current Operations Cell, examines data during a computer defense action in Europe. (U.S. Army photo.)



to exclude sources due to supply chain risk to a national security system or information technology item. The use of this authority by the head of a covered agency—for example, by the Secretary of the Army—must be based on a joint recommendation by the USD(AT&L) and the DOD Chief Information Officer, resulting from an intelligence-based risk assessment by the USD for Intelligence.

The USD(AT&L) must certify in writing, among other things, that use of this authority is “necessary to protect national security by reducing supply chain risk.” The Secretary of the Army cannot delegate this authority below the Army Acquisition Executive. Of note, no action taken under this authority shall be subject to review in a bid protest before the Government Accountability Office or in any federal court.

The Senate Armed Services Committee recommended this provision following submittal by DOD of a report to Congress on December 22, 2009, as required by Section 254 of the *Duncan Hunter National Defense Authorization Act for Fiscal Year 2009*. The Committee Report on the 2011 *NDAA* states, “The report found an increasing risk that systems and networks critical to DOD could be exploited through the introduction of counterfeit or malicious code and other defects introduced by suppliers of systems or components. The committee concludes that the Secretary [of Defense] should have the authority needed to address this risk.”

- Section 935, Reports on Department of Defense Progress in Defending the Department and the Defense Industrial Base from Cyber Events. This provision expresses congressional interest in and

THERE IS A RECOGNITION THAT FURTHER DOD GUIDANCE IS NEEDED TO ENSURE THAT PMS AND CONTRACTING OFFICERS HAVE THE TOOLS THEY NEED TO UNDERSTAND AND IMPLEMENT THIS POLICY.

concern about the threat to defense contractors’ networks. This section requires an annual report from the Secretary of Defense on DOD’s progress in defending the Department and defense contractors’ networks from cyber events.

One of the requirements of this provision is that the report include a description of the nature and scope of significant cyber events against the DIB during the preceding year, including the impact of such events on DOD generally and on operational capabilities; and, for any such event that has been investigated by or on behalf of the DOD Damage Assessment Management Office, a synopsis of each damage assessment report, with emphasis on actions needing remediation.

These assessments are done through the work of the DOD and the services’ damage assessment efforts within the DIB CS/IA Program, supported by subject-matter experts (SMEs) from affected acquisition program offices, and will be reported to Congress in classified form.

WHAT PEOS AND PMS SHOULD DO

DOD is maturing its capability to understand and mitigate the risk of losing of weapon system data. In the digitized, networked world, large quantities of program data reside on unclassified networks, and managing the risk to this information

is something that acquisition PMs must incorporate into their activities, drawing from the multilayered approach that DOD is developing.

PEOs, PMs, and other Army SMEs can draw from this maturing capability to enhance the security of their programs. For example, they should:

- Develop their program protection plans as early as possible in the acquisition cycle and maintain close collaboration with Army headquarters components that can facilitate this process, including conducting supply chain risk management assessments.
- Continually remind contractors’ project engineers with whom the PM team engages and shares digitized information about the importance of information assurance.
- Work with their contracting officer to use local contract clauses that reinforce the importance of protecting the most critical data held on contractors’ unclassified networks.
- Support requests to provide SMEs to execute the damage assessment process pursuant to DODI 5205.13.

PETER M. VELZ is Director, Acquisition Program Protection Policy in the Office of the ASAALT. He holds a B.B.A. in economics from Temple University and an M.A. in economics from the University of Connecticut.