April 8, 2011

Results in Brief: DoD Efforts to Protect Critical Program Information: The Air Force's Family of Advanced Beyond Line-of-Sight Terminals

What We Did

This is the second in a series of assessments to determine how DoD protects critical program information. The Air Force's Family of Advanced Beyond Line-of-Sight Terminals is the second of three acquisition category ID programs of record to be used as a case study to assess the Department's effectiveness in protecting critical program information. We conducted this assessment in coordination with DoD research, development, and acquisition, counterintelligence, and security subject matter experts. We assessed eight key issue areas related to program protection. Protecting critical program information is imperative in order for the U.S. to maintain the technologically-dependent cutting edge of its weapon systems.

What We Found

We found that while DoD and Air Force policy to protect critical program information has progressed in recent years, there is still a need for improvement. The Air Force has a good process in place for identifying critical program information through the use of an integrated product team. However, Air Force efforts to protect critical program information are not integrated and synchronized to the greatest extent possible, and they are not optimizing the ability to provide uniform research, development, and acquisition protection across the Air Force.

In addition, program officials were aware of horizontal protection but were utilizing an Air Force-developed database for horizontal protection purposes rather than the Acquisition Security Database managed by the Under Secretary of Defense for Acquisition, Technology, and Logistics. The workforce receives training in program protection; however, training needs to be more tailored. Program personnel used intelligence, counterintelligence, and security resources, threat data, and policies to guide program protection efforts; however, threat products were not timely, nor were they tailored to the critical program information. More coordination is needed among program, intelligence, counterintelligence, and security personnel – especially with Defense Security Service personnel – in order to optimize their efforts.

What We Recommend

The Office of the Under Secretary of Defense for Intelligence should strengthen policy related to critical program information protection in the area of tailoring threat products to ensure timeliness and relevance of the threat to program-specific critical program information. The Air Force should determine the most effective means to integrate and optimize Air Force research, development, and acquisition protection efforts.

Management Comments and Our Response

The Deputy Under Secretary of Defense for Intelligence and Security concurred with the recommendation and is in the final stages of promulgating policy and procedures to address the shortfall of threat product specificity and timeliness, with plans to publish a DoD Instruction 5240.LL, "Counterintelligence Activities in Research, Development, and Acquisition," by the third quarter of FY 2011. The Air Force also concurred and is in the process of integrating the key elements of DoD policy for the protection of critical program information by updating its "Program Protection Planning for Life Cycle Management" manual, with plans to publish the manual by the end of CY 2011