DSCA 00-07
Statement of Anti-Tamper (AT) Measures in the Letter of Offer and Acceptance (LOA)
16 May 2000

In reply refer to:
I-00/005895-PMD

Memorandum For Deputy Under Secretary of the Army (International Affairs)
Attn: SAUS-IA-DSZ
Department of the Army
Director, Navy International Programs Office
Department of the Navy
Deputy Under Secretary of the Air Force (International Affairs)
Department of the Air Force
Director, Defense Logistics Agency
Director, National Imagery and Mapping Agency
Director, Defense Threat Reduction Agency
Director, Defense Reutilization and Marketing Service
Director, Defense Information Systems Agency
Director, Defense Logistics Information Service
Deputy Director for Security Assistance,
Defense Finance and Accounting Service -- Denver Center

Subject: Statement of Anti-Tamper (AT) Measures in the Letter of Offer and Acceptance (LOA) (DSCA 00-07)

The co-development, sale or transfer of weapon systems to U.S. Allies and friends is sought by the Department of Defense to promote the goals of standardization, commonality, and interoperability with foreign governments currently or likely to become coalition partners. At the same time, the co-development, sale or transfer of weapon systems, and their potential loss on the battlefield will expose critical U.S. technology to potential exploitation or reverse-engineering attempts. To ensure the protection of selected critical technologies in U.S. weapon systems AT measures must be implemented.

AT measures are to be applied by those agencies involved in Foreign Military Sales programs and Direct Commercial Sales. AT measures, if determined to be required for a system, must be addressed in the LOA (see paragraph G.13. of the attached guidance). Specifically, maintenance and logistics restrictions due to AT must be stated in the LOA.

The attached *"Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs"*, issued by OUSD (AT&L) are effective immediately. If you have any questions regarding this matter, please feel free to contact Beth Baker (703) 604-6612/DSN 664-6612, e-mail: beth.baker@osd.pentagon.mil or Dawn Burke (703) 601-4464/DSN 664-4464, e-mail: dawn.burke@osd.pentagon.mil.

Attachment
OUSD (AT&L) Memorandum, 1 May 00, with Attachment

Guidelines for Implementation of Anti-Tamper Techniques in Weapon Systems Acquisition Programs
3 May 2000

The Under Secretary of Defense
3010 Defense Pentagon
Washington, D.C. 20301-3010

References:

(a) DoD 5200.1-M , *"Acquisition Systems Program Protection Plan"*

(b) Militarily Critical Technologies List

(c) DoD Department of Defense Directive Number 5200.39, Subject: *Security, Intelligence, and Counterintelligence Support to Acquisition Program Protection*

(d) *Technology Protection Handbook*

A. -- Purpose

Anti-Tamper (AT) measures are to be developed and implemented by the Acquisition Community involved in weapon systems programs. This guidance provides for the AT protection of selected critical technologies in U.S. weapon systems that may be developed with or sold to foreign governments or that may fall into enemy hands. These guidelines apply to system performance, materials, hardware, software, algorithms, design and production methods, maintenance and logistical support, and other facets as determined by competent acquisition authority. The DoD 5000 series will include provisions for incorporating AT into acquisition programs. Although protective in nature, AT will never be a substitute for appropriate physical security measures.

AT, if determined to be required for a system, must be reflected in the systems specifications, integrated logistics support plan, and other program documents. Because of its function, AT should not be regarded as an option or a system capability that may later be traded off without a thorough operational and acquisition risk analysis. User involvement will be pivotal to including AT in new programs, pre-planned product improvement (P3I), or technology insertion efforts. All Service, Defense Agency, and OSD comptrollers and financial management organizations must be involved in the coordination of program funding for AT and insure that funding or changes to funding are not made without proper justification based on risk analysis.

B. -- Applicability

This memorandum applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the Department of Defense Field Activities (hereafter referred to collectively as the "DoD Components"). This memorandum shall apply to all program categories of Department of Defense acquisition programs using critical technologies, whether the program is in development or undergoing P3I or other technology insertion. This memorandum will initially focus on tactical and strategic weapon systems. Revisions to the memorandum will be applicable to Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) and automated information systems acquisition programs. Program Managers of C4ISR and automated information systems acquisition programs are encouraged to assess their programs for inclusion of AT before being specifically required to do so.

C. -- Definitions and Acronyms:

Terms used in this memorandum are defined at Appendix 1.

D. -- Background:

1. The Department of Defense actively seeks to include foreign allies and friendly foreign countries as partners in the development, acquisition, and life-cycle management of weapon systems. Early involvement with foreign partners is encouraged by DoD, and such cooperative foreign government partnerships should begin at the requirements definition phase whenever possible. Successful execution of cooperative programs will promote the desirable objectives of standardization, commonality, and interoperability. The U.S. Government and its foreign government partners in these endeavors will benefit from shared development costs, reduced production and procurement costs realized from economies of scale, and strengthened domestic industrial bases. Similarly, the Department of Defense plays a key role in the execution of security cooperation programs which ultimately support national security objectives and foreign policy goals. U.S. weapon system sales are a major aspect of security cooperation. Anti-Tamper techniques and technologies allow the United States to meet foreign customer needs for advanced systems and capabilities, while ensuring the protection of U.S. technological investment and equities.

2. Increasingly, the U.S. Government relies on sophisticated technology in its weapons systems for effectiveness on the battlefield. Technology is today's and will be tomorrow's force multiplier, and technology improves survivability of the warfighter on the battlefield. It is prudent and practical to protect technologies deemed so critical that their exploitation will diminish or neutralize a weapon system's effectiveness. Protecting critical technologies preserves the U.S. government's resource investments in R&D as an investment, rather than as an expense, and enhances U.S. industrial base competitiveness in the international marketplace. The use of Anti-Tamper techniques and technologies is but one layer of protection that DoD programs will use to protect critical weapon system technologies.

E. -- Discussion:

1. Anti-Tamper encompasses the systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems. These activities involve the entire life-cycle of systems acquisition, including research, design, development, implementation, and testing of AT measures. Properly employed, AT will add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or system component. AT is not intended to completely defeat such hostile attempts, but it should discourage exploitation or reverse-engineering or make such efforts so time-consuming, difficult, and expensive that even if successful, a critical technology will have been replaced by its next-generation version. AT is intended to buy time for the U.S. and its allies to further develop critical technologies so that successful exploitation of earlier generations does not constitute a threat to their military forces and capabilities. AT can enhance the integrity of a system so that it performs as intended. The AT implementation will be evaluated during the program's developmental and operational testing through expert assessment. Exploitation by U.S national experts will be conducted during the verification and validation phase.

2. Anti-Tamper is the logical extension of a Program Protection Plan (PPP), described in reference B (DoD Dir 5200.39), and will be documented as a classified annex to the PPP. The AT annex will be updated with each PPP revision or P3I implementation. Note that a PPP is not required for every acquisition program, but the decision to exclude a PPP must be based on the technologies involved in the program. The DoD Technology Protection Handbook, the Defense Acquisition Deskbook, DoD 5000 series, and DoD 5200 series will include guidance on PPP and the AT annex in future revisions.

3. Programs will be evaluated in terms of the sensitivity of the technologies to be used. It is feasible that the evaluation may indicate that there is no requirement to protect the technologies planned or in use in the weapon system. The technology evaluation and assessment can be made by the Program Management Office preferably using qualified a disinterested third party (e.g., U.S. Government laboratory, Federally Funded Research and Development Center, or contractor preferably other than the Prime that does not have a conflict of interest). OUSD(AT&L) will review AT issues, decisions, and progress as a part of its normal program oversight responsibilities. A primary reference that the PM should use is the Militarily Critical Technologies List (MCTL) that can be accessed at http://www.dtic.mil/mctl. While the MCTL is an extensive listing, it is not comprehensive and may not have all technologies of interest listed. The technology assessment must specifically address the technology planned for inclusion in the program regarding whether it is listed in the MCTL. The Defense Technology Analysis Office is a resource for Program Managers, offering advice, assistance, and entree to other organizations that have AT capabilities. Appendix 2 provides a list of U.S. Government laboratories and their locations for Program Management Offices to use when considering use of AT measures.

F. -- Guidelines for Anti-Tamper Disclosure:

1. The fact that AT has been implemented in a weapons program should be unclassified unless the appropriate disclosure authority of the Component, in consultation with the program's MDA, has decided that the fact should be classified. The techniques and methods used to implement AT may be classified up to and including a Special Access Program (SAP) as appropriate. Classified AT information, including information concerning AT techniques and methods, will not be disclosed to any non-U.S. entity or person pursuant to disclosure decisions made in existing disclosure channels. Such disclosure decisions will take into account the opinions of the program's MDA and those of OUSD(AT&L). The program's MDA shall coordinate all foreign disclosure releases involving AT with the cognizant foreign disclosure office and security assistance office as appropriate. An Exception to National Disclosure Policy may be warranted for co-development programs, Foreign Military Sales, or Direct Commercial Sales.

G. -- Implementation:

1. AT is a systems engineering activity that must be initiated in program definition and risk reduction. AT is applicable to P3I upgrades or other technology insertion to fielded systems. AT requires resources and thus may affect other aspects of the program to include the cost and performance of the end product. AT involves risk analysis, and the decision not to implement AT must be based on operational risks involved as well as on acquisition risks including, but not limited to, feasibility, cost, system performance impacts, and schedule impacts.

2. AT shall be included in requirements development for all new acquisition programs effective with this memorandum. AT shall not be required for fielded systems or those that have passed Milestone II, because AT may be difficult or impossible to retrofit. However, AT shall be considered in any product improvement engineering effort for these systems. The use of AT may be required for programs, regardless of their acquisition status, at the discretion of the MDA.

3. AT shall be considered for use on any conventional system developed with allied partners, likely to be sold or provided to U.S. allies and friendly foreign governments, or likely to fall into enemy hands. If the system is not likely to be exposed to these scenarios, then AT may not be required. This decision, however, must be deliberate, fully supported, and documented in the PPP's AT annex.

4. U.S. weapon systems not intended for foreign distribution through FMS, DCS, or other avenues but that may fall into enemy hands on the battlefield shall include AT if critical technologies are involved.

5. The decision to use or not to use AT will be documented in a classified annex to the Program Protection Plan. The PM should consider using a qualified disinterested party to conduct the technology assessment and advise whether implementation of AT is required. The disinterested party may be a Federally Funded Research and Development Center, a

contractor that is free from conflict of interest, a university, or another Federal government agency. The Prime contractor may be used only if a qualified disinterested third party cannot be used.

6. If AT is determined necessary, the AT classified annex to the PPP will contain AT planning. The planning detail will correspond to the phase of the development of the program. The AT annex should also include, but is not limited to, the following information: identification of the critical technology being protected; how long AT is intended to delay hostile exploitation or reverse-engineering efforts; description of the planned AT approach; the effect compromise would have on the acquisition program if AT is not implemented; the estimated time and cost required for system or component redesign if compromise occurs; and the program's AT point of contact. The AT annex to the Program Protection Plan will be developed for Milestone II and updated at subsequent milestones.

7. AT applicability will be assessed for each major modification or P3I upgrade to the production system. It is feasible that AT may be inserted into the modified or upgraded systems if protection is required, or that AT may be discontinued when it is assessed that the technology no longer needs to be protected.

8. The recommendation to implement or not to implement AT will be approved by the responsible MDA. OUSD(AT&L) will keep abreast of AT as part of its program oversight role.

9. Service Acquisition Executives and OUSD(AT&L) shall be kept apprised of the status of AT in any program, including AT implemented in a SAP. Personnel in these offices shall be granted access to the SAP program in order to perform oversight functions should AT be implemented in a SAP program or should the AT itself require a SAP.

10. AT, whether implemented or not, will be a discussion item at Milestone II and Milestone III decision points. At Milestone II, AT shall be addressed in conceptual terms of how it is to be implemented; working prototypes appropriate to this stage of program development should be demonstrated. The Milestone III decision shall not be given favorable consideration until AT implementation is fully documented, tested during DT and OT, and ready for production.

11. Deliverables at Milestone II will include:

(1) a list of critical technologies;
(2) a threat analysis;
(3) identified vulnerabilities; and
(4) a preliminary AT requirement.

Deliverables at Milestone III will include:

(1) all deliverables from Milestone II and any updates;

(2) an analysis of AT methods that apply to the system, including cost/benefit assessments;

(3) an explanation of which AT method(s) will be implemented; and

(4) a plan for verifying and validating the AT implementation. These deliverables will be submitted as part of the AT annex to the PPP.

12. AT shall be verified and validated after weapon system implementation. This task shall be performed by a third party on actual or representative system components. The Verification and Validation (V&V) plan shall be reviewed at Milestone III. The V&V plan results shall be reported to the appropriate Service Acquisition Executive and OUSD(AT&L).

13. AT shall not be limited to developing and fielding a system. Equally important is life cycle management, particularly maintenance. Maintenance instructions and technical orders must clearly indicate that AT techniques have been implemented, the level at which maintenance is authorized, and warnings that damage may occur if improper or unauthorized maintenance is attempted. It may be necessary to limit the level and extent of maintenance a foreign customer may perform in order to protect critical technologies. This may mean that the level of maintenance that involves the AT will be accomplished only at the contractor or U.S. Government facility in the United States or overseas. Such maintenance restrictions may be no different than those imposed on U.S. Government users of AT protected systems. Maintenance and logistics restrictions must be stated in the appropriate contracts, PA, MOU, MOA, LOA, or other similar documents. The U.S. Government and U.S. industry must be protected against warranty and performance claims in the event AT measures are activated by unauthorized maintenance or other intrusion. Such unauthorized activities shall be regarded as hostile attempts to exploit or reverse engineer the weapon system or the AT technique itself and shall void warranties and performance guarantees.

14. Figure 1 is a representation of a generic decision process for implementing AT in a program. To fully support the systems engineering approach that defines the AT concept, participation of the acquisition program's Overarching Integrated Product Team (OIPT) is strongly recommended.

15. The Director, Strategic and Tactical Systems, will convene a standing OIPT to oversee and guide the use of AT in DoD acquisition programs and build a centralized AT technologies resource reference database for use by the acquisition community. The DoD Components and other organizations authorized to conduct acquisition development programs are encouraged to do likewise in coordination with OSD.

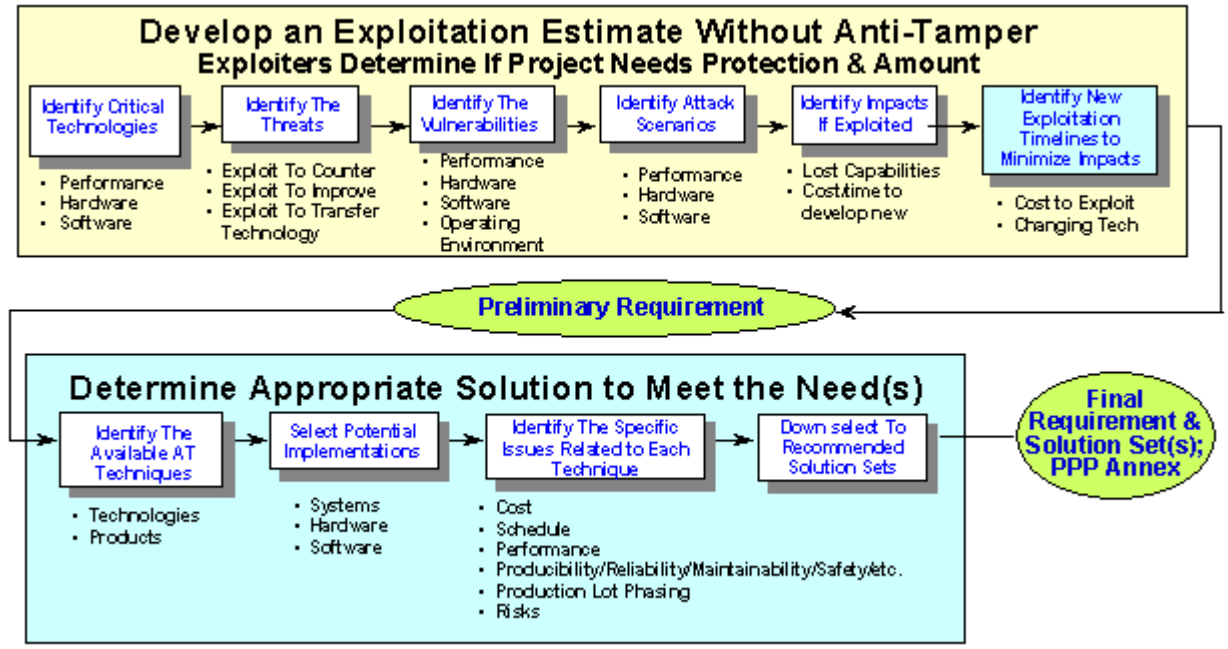

Figure 1 -- Anti-Tamper Implementation Decision Process

H. -- Supplement to the DoD Memorandum:

The DoD Components may supplement this memorandum, provided that any additional policies, directives, or related supplementing instructions do not contradict, negate, or otherwise lessen the intent and spirit of this memorandum. DoD Component supplements will be coordinated with OUSD(AT&L).

I. -- Review:

1. AT annexes will be reviewed and approved as a part of the Program Protection Plan. The Military Departments, Command, or Agency's Acquisition Executive and OUSD(AT&L) will be kept routinely apprised of AT implementation in development programs as well as in P3I to fielded systems as appropriate.

2. Any proposal to modify or change this memorandum must be approved by USD(AT&L).

/Signed/
J. S. Gansler

Appendix 1:

Definitions and Acronyms:

Anti-Tamper Techniques	Systems engineering activities intended to prevent and/or delay exploitation of critical technologies in U.S. weapon systems
AT	Anti-Tamper techniques
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DCS	Direct Commercial Sales
DoD	Department of Defense; the Department
FMS	Foreign Military Sales Program
LOA	Letter of Offer and Acceptance
MDA	Milestone Decision Authority
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
OIPT	Overarching Integrated Product Team
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics
PA	Project Arrangement
P3I	Pre-Planned Product Improvement
PEO	Program Executive Officer
PM	Program Manager
PPP	Program Protection Plan
SAP	Special Access Program
S&TS	Strategic and Tactical Systems
V&V	Verification and Validation

Appendix 2:

Program Managers AT Resources:

Laboratories. U.S. Government Laboratories are activities that perform one or more of the following functions: science and technology; engineering development; systems engineering; or engineering support of deployed materials and their modernization. The term includes laboratories; research institutes; and research, development, engineering, and technical activities. The following is a partial list of Department of Defense and Department of Energy laboratories and their locations that may potentially be of assistance to present and future weapon systems and other types of acquisition program Program Managers:

Office of the Secretary of Defense

1. Armed Forces Radiological Research Institute; Bethesda, MD

2. National Security Agency; Fort Meade, MD

3. Defense Technical Information Center Militarily Critical Technologies List (http://www.dtic.mil/mctl)

4. Defense Technology Analysis Office; Linthicum, MD

United States Army

1. Army Research Lab (ARL); Adelphi, MD

2. ARL; Aberdeen Proving Grounds, MD

3. ARL; White Sands Missile Range, NM

4. ARL, NASA; Langley, VA

5. ARL, NASA; Lewis, OH

6. Natick Research, Development, and Engineering Center; Natick, MA

7. Aviation Research, Development, and Engineering Center; St. Louis. MO

8. Aviation Troop Command, Aeroflight Dynamics Directorate; Moffett Field, CA

9. Aviation Troop Command, Aviation Applied Technology Directory; Fort Eustis, VA

10. Edgewood Research, Development, and Engineering Center; Aberdeen Proving Ground, MD

11. Communications Electronics Command Research, Development, and Engineering Center; Fort Monmouth, NJ

12. Communications Electronics Command Research, Development, and Engineering Center – Night Vision Electro-Optics Directorate, Fort Belvoir, VA

13. Missile Research, Development, and Engineering Center; Redstone Arsenal, AL

14. Armaments Research, Development, and Engineering Center; Picatinny Arsenal, NJ

15. Armaments Research, Development, and Engineering Center, Benet Labs; Watervliet Arsenal, NY

16. Tank-Automotive Command Research, Development, and Engineering Center; Warren, MI

17. USA Research Institute of Infectious Diseases; Fort Detrick, MD

18. Walter Reed Army Institute of Research; Washington, DC

19. Institute of Surgical Research; Fort Sam Houston, TX

20. Aeromedical Research Lab; Fort Rucker, AL

21. Medical Research Institute of Chemical Defense; Aberdeen Proving Ground, MD

22. Research Institute of Environmental Medicine; Natick, MA

23. Construction Engineering Research Laboratory; Champaign, IL

24. Cold Regions Research and Engineering Lab; Hanover, NH

25. Topographic Engineering Center; Alexandria, VA

26. Waterways Experiment Station; Vicksburg, MS

27. Research Institute for Behavioral and Social Sciences; Alexandria, VA

28. Simulation, Training, and Instrumentation Command; Orlando, FL

29. High Energy Laser Systems Test Facility; White Sands Missile Range, NM

United States Navy

1. Naval Air Warfare Center, Weapons Division; China Lake, CA

2. Naval Air Warfare Center, Weapons Division; Point Mugu, CA

3. Naval Air Warfare Center, Aircraft Division; Patuxent River, MD

4. Naval Air Warfare Center, Aircraft Division; Lakehurst, NJ

5. Naval Research Lab; Washington, DC

6. Naval Research Lab Detachment; Bay St. Louis, MS

7. Naval Surface Warfare Center, Carderock Division; Bethesda, MD

8. Naval Surface Warfare Center, Crane Division; Crane, IN

9. Naval Surface Warfare Center, Dahlgren Division; Dahlgren, VA

10. Naval Surface Warfare Center, Dahlgren Detachment; Panama City, FL

11. Naval Surface Warfare Center, Indian Head Division; Indian Head, MD

12. Naval Surface Warfare Center, Port Hueneme Division; Port Hueneme, CA

13. Naval Surface Warfare Center; Bayview, ID

14. Naval Command, Control, and Ocean Surveillance Center; San Diego, CA

15. Naval Command, Control, and Ocean Surveillance Center, In-Service Engineering Division; Charleston, SC

16. Naval Command, Control, and Ocean Surveillance Center, In-Service Engineering Division; Pearl Harbor, HI

17. Naval Aerospace Medical Research Center; Pensacola, FL

18. Naval Dental Research Lab; Great Lakes, IL

19. Naval Health Research Center; San Diego, CA

20. Naval Undersea Warfare Center, Keyport Division; Keyport, WA

21. Naval Surface Warfare Center, Carderock Division, Philadelphia Det.; Philadelphia, PA

22. Naval Undersea Warfare Center; Newport, RI

23. Naval Research Lab, Monterey Detachment; Monterey, CA

24. Naval Air Systems Command (engineering functions)

25. Naval Sea Systems Command (engineering functions)

26. Naval Air Warfare Center Training Systems Division; Orlando, FL

27. Naval and Clothing Textile Research Facility; Natick, MA

28. Naval Facilities Engineering Service Center; Port Hueneme, CA

29. Naval Submarine Medical Research Laboratory; Groton, CT

30. AEGIS; Wallops Island, VA

31. AEGIS; Morristown, NJ

32. Naval Warfare Assessment Division; Corona, CA

33. Explosive Ordnance Disposal Technical Center; Indian Head, MD

34. Naval Ordnance Center; Indian Head, MD

35. Naval Sea Logistics Center; Mechanicsburg, PA

36. Fleet Technical Support Center; Mayport, FL

37. Fleet Technical Support Center; San Diego, CA

38. Fleet Technical Support Center; Pearl Harbor, HI

United States Air Force

Air Force Anti-Tamper POC is SAF/AQL, 703-588-1630, DSN 425-1630.

1. Air Force Research Laboratory; Wright-Patterson AFB, OH
Operating Locations:

   a. Wright-Patterson AFB, OH
   b. Brooks AFB, TX
   c. Mesa, AZ
   d. Eglin AFB, FL
   e. Tyndall AFB, FL
   f. Kirtland AFB, NM
   g. Hanscom AFB, MA
   h. Edwards AFB, CA
   i. Griffiss AFB, Rome, NY

2. Aeronautical Systems Center; Wright-Patterson AFB, OH (engineering functions)

3. Electronic Systems Center; Hanscom AFB, MA (engineering functions)

4. Space and Missile Center; Los Angeles AFB, CA (engineering functions)

5. Air Armament Center; Eglin AFB, FL (engineering functions)

6. Oklahoma City Air Logistics Center; Tinker AFB, OK (engineering functions, minus supply, depot maintenance, and host base support)

7. Ogden Air Logistics Center; Hill AFB, UT (engineering functions, minus supply, depot maintenance, and host base support)

8. Warner-Robbins Air Logistics Center; Robbins AFB, GA (engineering functions, minus supply, depot maintenance, and host base support)

Department of Energy

1. Sandia National Laboratories: Kirtland AFB, NM

2. Los Alamos National Laboratory; Los Alamos, NM

3. Lawrence Livermore National Laboratory; Livermore, CA