SSAA OUTLINE{tc "E6. ENCLOSURE 6SYSTEM SECURITY AUTHORIZATION AGREEMENT (SSAA) OUTLINE"}

The SSAA is a living document that represents the formal agreement among the DAA, the CA, the user representative, and the program manager. The SSAA is developed in phase 1 and updated in each phase as the system development progresses and new information becomes available. At minimum, the SSAA should contain the information in the following sample format:

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
   - 1.1. System name and identification.
   - 1.2. System description.
   - 1.3. Functional description.
     - 1.3.1. System capabilities.
     - 1.3.2. System criticality.
     - 1.3.3. Classification and sensitivity of data processed.
     - 1.3.4. System user description and clearance levels.
     - 1.3.5. Life-cycle of the system.
   - 1.4. System CONOPS summary.

2. ENVIRONMENT DESCRIPTION
   - 2.1. Operating environment.
   - 2.2. Software development and maintenance environment.
   - 2.3. Threat description.

3. SYSTEM ARCHITECTURAL DESCRIPTION
   - 3.1. Hardware.
   - 3.2. Software .
   - 3.3. Firmware .
   - 3.4. System interfaces and external connections.
   - 3.5. Data flow (including data flow diagrams).
   - 3.6. TAFIM DGSA, (reference (o)), security view.
   - 3.7. Accreditation boundary.

4. ITSEC SYSTEM CLASS
   - 4.1. Interfacing mode.
   - 4.2. Processing mode.
   - 4.3. Attribution mode.
   - 4.4. Mission-reliance factor.
   - 4.5. Accessibility factor.
   - 4.6. Accuracy factor.
   - 4.7. Information categories.
   - 4.8. System class level.

4.9. Certification analysis level.

5. SYSTEM SECURITY REQUIREMENTS
   5.1. National and DoD security requirements.
   5.2. Governing security requisites.
   5.3. Data security requirements.
   5.4. Security CONOPS.
   5.5. Network connection rules.
      5.5.1. To connect to this system.
      5.5.2. To connect to the other systems defined in the CONOPS.
   5.6. Configuration and change management requirements.
   5.7. Reaccreditation requirements.

6. ORGANIZATIONS AND RESOURCES
   6.1. Identification of organizations.
      6.1.1. DAA.
      6.1.2. CA.
      6.1.3. Identification of the user representative.
      6.1.4. Identification of the organization responsible for the system.
      6.1.5. Identification of the program manager or system manager.
   6.2. Resources.
      6.2.1. Staffing requirements.
      6.2.2. Funding requirements.
   6.3. Training for certification team.
   6.4. Roles and responsibilities.
   6.5. Other supporting organizations or working groups.

7. DITSCAP PLAN
   7.1. Tailoring factors.
      7.1.1. Programmatic considerations.
      7.1.2. Security environment.
      7.1.3. IT system characteristics.
      7.1.4. Reuse of previously approved solutions.
      7.1.5. Tailoring summary.
   7.2. Tasks and milestones.
   7.3. Schedule summary.
   7.4. Level of effort.
   7.5. Roles and responsibilities.

Appendices shall be added to include system C&A artifacts. Optional appendices may be added to meet specific needs. Include all documentation that will be relevant to the systems' C&A.

APPENDIX A. Acronym list
APPENDIX B. Definitions
APPENDIX C. References
APPENDIX D. Security requirements and/or requirements traceability matrix
APPENDIX E. Security test and evaluation plan and procedures
APPENDIX F. Certification results
APPENDIX G. Risk assessment results
APPENDIX H. CA's recommendation
APPENDIX I. System rules of behavior
APPENDIX J. Contingency plan(s)
APPENDIX K. Security awareness and training plan
APPENDIX L. Personnel controls and technical security controls
APPENDIX M. Incident response plan
APPENDIX N. Memorandums of agreement - system interconnect agreements
APPENDIX O. Applicable system development artifacts or system documentation
APPENDIX P. Accreditation documentation and accreditation statement