

## RESOURCES FOR ASSISTANCE IN DEVELOPING AN ACCESS CONTROL PLAN/TECHNOLOGY CONTROL PLAN

An “**Access Control Plan/Technology Control Plan**” (ACP/TCP) is a written documented plan developed to prevent the unauthorized export or disclosure of technical data, regardless of whether in the U.S. or abroad, to unauthorized U.S. citizens, and to any foreign concern, foreign interest, foreign national, or their representatives (U.S. citizens or otherwise), including those who are its own agents or employees.

Per the NISPOM Section 2-307, the ACP/TCP shall prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. The ACP/TCP shall also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate Federal Government disclosure authorization has been obtained; e.g., an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures shall be included, as appropriate.

If you are eligible to receive access to Naval Nuclear Propulsion Information (NNPI) and expect to have a “need to know” for NNPI, your ACP/TCP should address the more stringent requirements for controlling NNPI identified in NAVSEAINST 5511.32 (applicable revision); NAVSEA 5252.227-9100, Protection of Naval Nuclear Propulsion Information, and NAVSEA 5252.227-9101, Transmission Abroad of Equipment or Technical Data Relating to the Nuclear Propulsion of Naval Ships.

### Web Sites:

Although there may be others, the following resources provide useful help and guidelines in establishing an ACP/TCP and an Import/Export Control and Compliance Program.

- U.S. State Department, DDTC  
<http://www.pmdtc.state.gov/compliance.htm>  
To ensure compliance with U.S. export law and regulations, the Directorate of Defense Trade Controls (DDTC) strongly advises that registered exporters and manufacturers have in place programs that assist in monitoring defense trade activities.  
DDTC has outlined some elements that it believes should be included in a compliance program: [Guidelines for DDTC Registered Exporters/Manufacturers Compliance Program](#)  
These programs should include a manual that articulates the company's policy on and commitment to compliance with defense trade laws and regulations, and that outlines the procedures for dealing with licensing and compliance matters. Such a manual should also include the identification and duties of empowered and responsible persons, and procedures on record keeping and internal auditing.
- U.S. Department of Commerce, Bureau of Industry and Security, “Export Management Systems (EMS) Guidelines”  
<http://www.bis.doc.gov/ComplianceAndEnforcement/ExportManagementSystems.htm>  
BIS has published the [EMS Guidelines](#) (The Guidelines) to assist companies in establishing internal control procedures for vigilant screening of export/re-export transactions. The Guidelines provide ideas, examples of best practices and tools that have proven effective in U.S. businesses.
- Control Procedures for Unclassified Technical Data Disclosing Militarily Critical Technology (pertaining to the DLIS U.S./ Canada Joint Certification Program)  
<http://www.dlis.dla.mil/jcp/documents.asp>
- Control of Naval Nuclear Propulsion Information (NNPI)  
NAVSEAINST 5511.32 – (Contact Buyer. Not available on public Web Site)
- Defense Security Service (DSS)  
National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M, Section 2.307, Technology Control Plan (TCP)  
Sample TCP refer to [http://www.dss.mil/isp/foci/sample\\_tech\\_con\\_plan.html](http://www.dss.mil/isp/foci/sample_tech_con_plan.html)