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

Updated 12/9/13

Electric Boat requires that suppliers have an Access Control Plan or Technology Control Plan (ACP/TCP) if they will require access to export controlled equipment, technical data or information.

An ACP/TCP is a written documented plan developed to prevent the unauthorized export or disclosure of export controlled equipment or 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).

Not all ACP/TCPs are the same. Your ACP/TCP should be tailored to suit your organization.

The following selected resources provide useful help and guidelines in establishing an ACP/TCP:

U.S. State Department, DDTC
http://www.pmddtc.state.gov/compliance/index.html
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 programs that assist in monitoring defense trade activities.

DDTC Compliance Program Guidelines:
http://www.pmddtc.state.gov/compliance/documents/compliance_programs.pdf
A strong compliance program 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 recordkeeping and internal auditing.

Defense Logistics Information Service (DLIS)
The DLIS plays a major role in establishing a U.S. or Canadian company's eligibility for militarily critical technical data through the U.S./Canada Joint Certification Program. The following DLIS publication offers guidance on protecting militarily critical technical data:
Control Procedures for Unclassified Technical Data Disclosing Militarily Critical Technology
http://www.dlis.dla.mil/JCP/forms/Control_Procedures.pdf

Defense Security Service (DSS)
National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M, Section 2.307, Technology Control Plan (TCP)
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.

Sample ACP/TCP - see http://www.dss.mil/isp/foci/sample_tech_con_plan.html

Naval Nuclear Propulsion Information (NNPI)

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 OPNAVINST N9210.3; 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.