

BACKGROUND AND KEY PROVISIONS OF THE TECHNOLOGY SECURITY ACT **Introduced by Rep. Howard Berman (D-CA)**

BACKGROUND

The Technology Security Act is the first complete revision since 1979 of U.S. controls on the export of “dual-use” items, services and technological information. The existing statute, the Export Administration Act (EAA), lapsed from 1994 to 2000 and again from 2001 to the present. Presidents Clinton, Bush and Obama have invoked emergency Presidential authority to keep the regulations in effect through a series of Executive Orders. Legislative proposals from 1990 to 2001 would have amended, but not rewritten, the old EAA.

The EAA is an artifact of the Cold War. It is focused on preventing the Soviet Union, China and the Warsaw Pact from obtaining Western goods and manufacturing technology that could be used for improving their military and for modernizing their economies. The EAA was written when the U.S., Europe and Japan shared a common export control policy and when sensitive technology was concentrated in a few countries and thus controllable. None of those conditions exist today.

KEY PROVISIONS

- In contrast to the highly-prescriptive and static EAA, the bill provides the President with broad and flexible authority to deploy controls to counteract current and future national security threats, including rogue governments, terrorist organizations, and other non-state actors that seek to attack the U.S. and its allies.
- The bill modernizes the definition of national security to include sustaining U.S. leadership in science, manufacturing and our high-tech workforce, and requires the President to balance traditional security goals with maintaining U.S. academic and manufacturing leadership in applying controls.
- In recognition that knowledge of sensitive technology can be as threatening as dual-use goods, the bill expands the scope of controls to include transfer of information via the Internet.
- The bill updates the scope of threats against which controls can be utilized to include cyber attacks on critical data systems, attacks on U.S. infrastructure and protection of critical scientific and industrial facilities.
- The bill strengthens the policy-making on controls by establishing a high-level interagency management group, with ongoing responsibility for overall administration, rule-making and oversight of controls. This addresses a long-standing weakness caused by the current ad-hoc policy-making structure.
- The bill re-enacts provisions authorizing anti-boycott authority and non-proliferation functions of the U.S. government.

