soundmasking.com by DYNASOUND

eavesdropping protection systems

designed for today, engineered for tomorrow

soundmasking solutions
to protect sensitive and
confidential conversations

Dynasound, Inc. 6439 Atlantic Blvd. Norcross, GA. 30071
800-989-6275 www.soundmasking.com

Threat Analysis

When the area of concern is viewed as a six sided enclosure, the breach points can be easily identified; windows, walls, doors, ducts and utility penetrations. A properly designed audio security system protects against inadvertent and deliberate eavesdropping attempts.

- Laser listening devices are sometimes used to capture conversations from vibrations on window surfaces.
- Ductwork can be used to listen-in on conversations from several offices away or to hide listening devices.

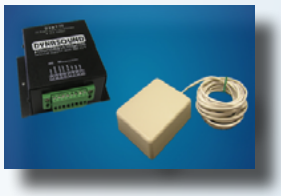
- Doors are an obvious point of vulnerability for eavesdroppers or passers-by.
- Ceiling plenums and open return-air grills allow conversations to travel between rooms.
- Electrical conduit is a possible sound path exiting the secure space.
- Raised access floors are highly reverberant environments that can easily transmit sound between offices.

Dynasound, Inc. 6439 Atlantic Blvd. Norcross, GA. 30071
800-989-6275 www.soundmasking.com

The Solution

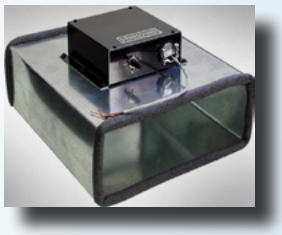
Since 1975 Dynasound has been the leading innovator in the field of electronic sound masking. Audio surveillance countermeasures, or eavesdropping protection, through the use of engineered sound is one such advancement. These solutions are regularly used to protect corporate intellectual property, mission critical conversations and national security.
Dynasound provides 70.7 volt based systems as well as state of the art networked security soundmasking systems.

Typical Breech Points Protected



Doors: Door maskers provide protection from intentional eavesdroppers by applying low-level soundmasking to the door surface, filling the gaps around the door and door frame with protective sound.

Windows: Windows present both visual and acoustical breech points. With only visual access to the facility, sensitive laser devices and parabolic microphones can capture conversations at great distances.



HVAC ducts: Metal ductwork creates a highly reverberant path that carries conversations far beyond the intended perimeter. Dynasound's duct masking devices are installed without any penetration into the duct it's self, masking conversation without impeding air flow.

Walls and Wall penetrations: Any utility penetration creates a breech point. Pipes and conduits may transmit sound from the secured space. Even without utility penetrations an unmasked wall can be vulnerable to contact microphones and listening devices.

Perimeter areas: In many cases the most effective way to prevent unintentional or accidental eavesdropping is to add conventional soundmasking to the perimeter area surrounding the secured space.

Ceiling plenums and Raised access floors: Reverberant cavities above and below office walls can easily transmit sound from one space to another.

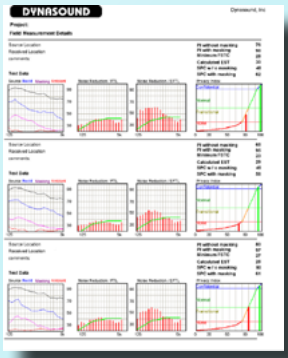
Portable Eavesdropping Protection

When a SCIF (Sensitive Compartmentalized Information Facility) is not available, confidential speech privacy is still attainable with Dynasound's PEP Pack. The Portable Eavesdropping Protection system comes complete and ready to travel.

- Uses the same technology as many permanent SCIFs
- Plug and play connections; uses easy to setup and remove attachments.
- Custom configurations and military spec Pelican® cases

Testing and Reporting

- **FSTC** (Field Sound Transmission Class)
- **PI** (Privacy Index)
- **SPC** (Speech Privacy Class)



Dynasound provides testing services based on ASTM standards and uses state of the art equipment. Using Larsen Davis sound level meters and dodecahedron sound sources Dynasound can measure and document Field Sound Transmission Class, Privacy Index and Speech Privacy Class ratings.

Since 1975, Dynasound has secured the confidential speech privacy of many government and corporate facilities by designing and implementing soundmasking solutions to guard against eavesdropping. Our audio security clients include government agencies, defense contractors, miltary bases, senior level corporate offices, boardrooms and research & development facilities. Below are a few of our clients:

Aerojet Electric Sytems
Allied-Signal
Arnold AFB/RDC
AT&T Tech./Guilford Center
Argonne National Labs
BAE Systems
Bank of America
Bellsouth
BF Goodrich Aerospace
Boeing
Booze Allen & Hamilton
Brown & Root
Center for Disease Control
CitiGroup
Coca-Cola
Defense Intelligence Agency
Edwards AFB
Environment Research Institute
Ernst & Young
Falcon Air Station
Federal Communications Commission
Federal Reserve Bank
Fleet Bank
Ford Motor Company
Fort Belvoir
Fort Ritchie
Fort McPerson
Georgia Tech Research Institute
General Electric / Neutron Systems
General Dynamics
GTE
Hill AFB
Hewlett Packard
Honeywell Defense Systems
IBM
Kaiser Permanente
Kirtland AFB
Los Alamos Labs
Lockheed Martin
Magnovox Electric Systems
Malstrom AFB
Motorola
National Security Agency
Naval Air Engineering
Naval Intelligence Center
Naval Sea Command
NORAD
Northrup Grumann
Pfizer
Phillips Labs
PricewaterhouseCoopers
Proctor & Gamble
Raytheon
Rockwell International Science Center
Sandia National Labs
Space Command Headquarters
Stategic Air Command
Texas Instruments
TRW
Upjohn
U.S. Army Research Center
U.S. Army Tank Command
U.S. Navy / Point Magu, CA
U.S. Navy / Norfolk, VA
U.S. Navy / Warminster, PA
United Technologies / Adv.Sys.Div.
Vandenburg AFB
Wright Patterson AFB
3M