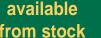
## **CNS7109**

### COAXIAL AMPLIFIED NOISE SOURCE



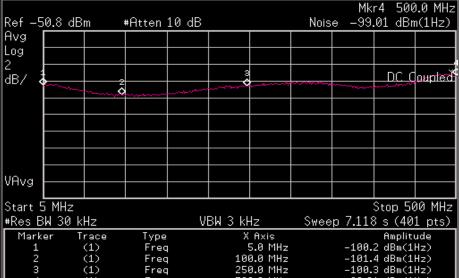
-101.4 dBm(1Hz) -100.3 dBm(1Hz)

-99.01 dBm(1Hz)



# +12V G 54487 MICRONETICS CNS7109-D1C DC 0604 SN ENG

# **CNS7109 Typical Data**



500.0 MHz

#### **SPECIFICATIONS**

• Frequency: 5 MHz to 500 MHz

(1) (1)

• Noise Power Spectral Density (No): -103 dBm/Hz (min)

Freq

Freq

• Noise Power (N): -16 dBm

• Spectral Flatness: 3 dB (total window)

· Bias: 12 Vdc, Internally Regulated

• Current Draw: 50 mA Max

Peak Factor:

• Operating Temp: -55 to +85 C • Storage Temp: -55 to 125 C

### **5 MHz** TO **500 MHz**

#### **DESCRIPTION**

The CNS7109 noise module is designed for a wide range of applications. It features high noise output amplitude for uses ranging from encryption to jamming. All biasing and amplification circuitry is built-in making it easy to design into your system. It features a built-in voltage regulator for highly stable output even if your DC supply lines are not.

#### **APPLICATIONS**

Common Noise Applications

#### 1. Built-in IF Testing:

Highly stable flat over frequency noise sources serve to provide built-in test for an IF subsystem. By injecting a stable signal reference through the IF chain, one can calibrate the gain/loss and frequency response. In addition, the noise source can be used to set up Eb/No for built-in stimulated BER testing of digital demodulation.

#### 1. Barrage Jamming:

The noise source is fed into the tuning port of a VCO via a bias tee and a positive DC voltage. The random nature of noise makes the output of the VCO to hop around in a given frequency band randomly making an ideal jamming signal. Further circuitry can be used between the noise source and tuning port to shape the noise probability density function (PDF) for the desired jamming effect.

#### 2. Random Number Generation for Encryption:

Noise sources being truly random (not pseudorandom) give the ultimate in secure communication because of their ability to generate a truly random number pattern. This can be used to seed an encryption key for authentication. The noise signal can be fed directly into an A/D converter for sampling or a simpler techniques might use a comparator. Further shaping of the noise is often employed whether either analog if in front of the A/D converter or afterwards using DSP.



