



FOR IMMEDIATE RELEASE

CONTACTS: For Financial Press
Ned Mavrommatis
Chief Financial Officer
ned@id-systems.com
General Phone: 201-996-9000.

For Trade Press
Greg Smith
Director of Marketing
gsmith@id-systems.com
General Fax: 201-996-9144

Transportation Security Administration Awards I.D. Systems Follow-On Grant

Wireless Vehicle Security & Management System to be Deployed at Jacksonville Seaport

Hackensack, N.J., July 7, 2004 —

I.D. Systems, Inc. (NASDAQ: IDSY) today announced that it has been awarded a grant by the Transportation Security Administration (TSA) to implement the company's Wireless Asset Net™ vehicle security and management system at JAXPORT, the Jacksonville, Fla., seaport operated by the Jacksonville Port Authority. I.D. Systems previously deployed a similar system at Newark Liberty International Airport. The new TSA grant is for \$1.36 million for Phase I to be completed in 2004. Additional funding can be provided for Phase II system expansion, which would be initiated at the TSA's discretion in fiscal year 2005 for an additional \$1.35 million.

The previous TSA program with I.D. Systems at Newark Airport established the viability of the Wireless Asset Net for deployment on airport equipment — specifically vehicles operating in the secure airside area of operations. The more extensive system deployment slated for JAXPORT is expected to validate system benefits on a larger scale and in a different, though related, environment, thereby providing port authorities and shipping companies with the proof of concept data necessary to move forward with broader implementation of wireless fleet security and management. JAXPORT has entered into a Memorandum of Understanding with the TSA to become the first seaport to participate in this vehicle security demonstration.

“We are very excited that the TSA has awarded I.D. Systems a new program to continue deploying our vehicle management technology for homeland security applications,” said Rick Muntz, I.D. Systems' executive vice president of sales, marketing, and customer satisfaction. “This latest grant reflects the unique advantages our system has over the many technologies competing for TSA funding. For example, unlike other approaches to vehicle control and monitoring, which depend heavily on constant wireless network connectivity and continuous communication with a single central control point, our patented system of ‘distributed intelligence’ is designed to enable autonomous hardware and software onboard each vehicle to perform critical tasks without regard to network status – and with no single point of system failure. This is a vital capability during emergencies, when communication networks can quickly become overburdened, even useless, as we saw happen to cellular networks on 9/11.”

“In addition,” continued Mr. Muntz, “the migration of our vehicle management solutions to JAXPORT opens up the seaport vehicle security market as another new application of our technology. We view this as another significant opportunity for revenue growth, above and beyond the airport vehicle security market.”

About The Wireless Asset Net

The Wireless Asset Net system represents a last line of defense against security breaches involving airport and seaport ground vehicles. The system provides vehicle security, improves fleet manageability, and reduces traffic congestion by incorporating the following functions and benefits:

- Vehicle-operator assignments established and updated remotely via system software link to security and training systems
- Vehicle traffic mapping and monitoring, via local RF wireless network and wide-area GPS location monitoring
- Historical capture of vehicles movements for incident investigations
- Geo-fencing, with alarms for defined transgressions (e.g. travel into unauthorized zones) and potential ability to disable vehicles remotely
- Improved vehicle utilization and fleet size optimization to reduce fleet operating costs and traffic congestion
- Improved operator accountability for use of vehicles, including impact sensing, to reduce accident costs, improve safety on port property, and increase the useful life of equipment
- Improved maintenance controls, including electronic vehicle inspection checklists and detection/upload of actual vehicle run-time, to improve the preventative maintenance process and reduce maintenance costs
- Automatic OSHA compliance, including electronic vehicle inspection checklists and vehicle access control linked to operator training, to satisfy regulatory requirements, improve worker safety, and reduce associated costs
- Improved vehicle dispatching through two-way communications with vehicles/operators to increase operational efficiency and help optimize fleet size

About I.D. Systems

Based in Hackensack, N.J., I.D. Systems, Inc. is a leading provider of wireless solutions for corporate asset management. I.D. Systems' customers include 3M Company, American Axle, Archer Daniels Midland, Daimler Chrysler, Deere & Co., Ford Motor Company, General Dynamics, Hallmark Cards, Northrop Grumman, Target Corporation, Walgreen Co., the U.S. Navy, the U.S. Postal Service, and the Transportation Security Administration, among others. Using local area networks, wide area networks, and the Internet, the company's systems enable management to control and track the location and status of their assets — from forklifts, tugs and cranes to automobiles and trucks — in real time. For more information on I.D. Systems, Inc., visit www.id-systems.com.

“Safe Harbor” statement under the Private Securities Litigation Reform Act of 1995: This press release contains forward looking statements that are subject to risk and uncertainties, including, but not limited to, the impact of competitive products, product demand and market acceptance risks, fluctuations in operating results and other risks detailed from time to time in I.D. Systems' filings with the Securities and Exchange Commission. These risks could cause I.D. Systems' actual results for the current fiscal year and beyond to differ materially from those expressed in any forward looking statements made by, or behalf of, I.D. Systems.

#