

Corporate Security

Biweekly Intelligence Tracking Cutting-Edge Practices, Trends And New Technologies For Security Executives

Unified Access Card May Be Used For Systems

Stanley Security Solutions/Indianapolis is gratified for a federal regulation requiring use of smart cards by many government employees.

The company recently got a \$4.8 million contract to install access control equipment and servers for a smart card system regulating all NASA buildings.

"The contract that we just won was for all the field equipment," said **Joe Costa**, VP of sales for Stanley Security. It includes "all the door controllers, the devices that the smart card readers would attach to and the intelligent panels that would run [access control] in the building and that would terminate back to a regional server and then an enterprise server." The enterprise server was installed in Huntsville, Ala.

"This card can be used not only for identification purposes and physical access to doors, but also on the 'logical access' side, which would allow ac-

cess to systems and databases as well," Costa added. NASA plans to take the next step up from smart cards to logical access in the future, he said, although that transition is not part of the current contract.

Benefits of a common badging/access control system lie in cost savings and ease of use for both employees and operators.

Fewer security staff are needed to run the unified system from a single central command center, and buying equipment and cards in bulk drives down acquisition costs.

Plus, the system makes it easy for security to obtain an audit trail of an employee's movement from building to building, Costa said, as that information is deposited in a common database rather than multiple databases.

And, security departments benefit from the ease of terminating card privileges after an employee is fired or resigns. ●