cameras using a mixture of wireless and fiber optic technologies, along with gunshot detection software and facial recognition analytics.

To fund that expansion, the city will be looking for other grants. In doing so, it will be able to point to the success of the current system and the adoption of the common vision of the city's citizens, business owners and politicians.

Still, if I had to point to one thing that made this all a success, it would be taking the time to talk with everyone in the community and listening to their concerns, hopes and dreams — then putting those thoughts into a single vision and goal that everyone can embrace. ▮

*Tyrone (Ty) Morrow served as the chief of police for Bryan, Texas from 2007 until he retired earlier this year. During that time, he oversaw the installation of a wireless public safety camera system in downtown Bryan. Morrow's next venture is to head to the Middle East to help train police officers in Abu Dhabi, the capital of the United Arab Emirates.*



## Compliance Scorecard

Security Leadership Solutions Executive Council

# Keep an Eye on ICE

By Marleah Blades

Security breaches in federal information networks are not just the stuff of spy movies and conspiracy theorists. In December of last year, the Cybersecurity Commission of the Center for Strategic and International Studies reported that 2007 saw several major intrusions by foreign entities, and this year we have seen reports of network intruders accessing data from the Pentagon, the FAA and the U.S. Air Force. A burst of DoS attacks on South Korean and U.S. government Web sites in July brought the issue to the forefront again this summer, prompting Senator Thomas Carper (D-DE) to call again for the passage of S.921, a bill he introduced in April.

Otherwise known as the U.S. Information and Communications Enhancement (ICE) Act, the bill would amend the Federal Information Security Management Act (FISMA) to require agencies to continually monitor their networks for incidents, address vulnerabilities and regularly test the measures in place. It would also require agencies to purchase more secure hardware and software and to develop policies for coordinating with US-CERT. As other recent legislation has done, the ICE Act advocates the creation of a cyber security office that reports directly to the President.

Carper and many others within and outside of the government believe FISMA in its current form acts more as a checklist and a driver of paperwork than a truly effective measure of the quality of information security. At a presentation at the RSA Conference in April, Eric Hopkins, a staff member with the Senate Committee on Homeland Security and Governmental Affairs, said that reforming FISMA would result in economies of scale, more coordinated security efforts, and stronger information security overall.

The ICE Act, if passed, would clearly change the way government agencies deal with and assess information security.

*Marleah Blades is senior editor for the Security Executive Council (SEC). The Security Executive Council maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). Help the Council fill out the list and receive a selected complimentary metric slide from our store.*