Homeland Security
Science and Technology

# Highlight

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems, and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency responder equipment;
- Providing information that enables decision makers and responders to better select, procure, use, and maintain emergency responder equipment.

Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to federal, state, and local responders.

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

To contact the SAVER Program Support Office
Telephone: 877-336-2752
E-mail: saver@dhs.gov
Visit SAVER on the RKB Web site:
https://www.rkb.us/saver

## Encryption-Software

Emergency responders rely on digital communications to share information for many public safety missions, including crime incident response, fire incident response, medical emergency response, emergency management, mutual aid, and task force operations. The data being shared may contain sensitive information; therefore, emergency responders require data protection to mitigate security risks and prevent the misuse of information. Encryption software protects digital communications, such as e-mail and instant messaging, from individuals not authorized to handle such data. This type of protection, if properly implemented, allows a community to share sensitive information more readily, ensuring that information will only be received or viewed by authorized personnel.

As a SAVER Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN), Charleston has been tasked to provide expertise and analysis on key subject areas including communications, sensors, perimeter security, weapon detection, and surveillance, among others. In support of this tasking, SPAWARSYSCEN has executed a project and produced the following reports that will provide the emergency responder community with specific information on the technologies, capabilities, and limitations of encryption software tools:

The Encryption Software Market Survey Report identifies commercial off-the-shelf (COTS) encryption software tools and provides a useful starting point for the emergency responder community during evaluation and procurement of encryption software tools. Findings presented in this document are the result of extensive Web-based research, focus group discussions, practitioner interviews, and manufacturer responses to a Request for Information (RFI). This report is comprised of vendor-provided software application capability information and additional product information collected from the software vendor community.

The Encryption Software Tools Technology Guide incorporates the critical operational, functional, and technical requirements that are essential for a successful encryption system. The intended audience of this document includes incident commanders and Information Technology (IT) managers within emergency response organizations.

The *Encryption Software Purchase and Implementation Guide* is designed to provide the emergency responder community, most notably, incident commanders and IT management, with user needs, initial evaluation criteria, and implementation considerations to initiate their assessment of encryption software solutions. A four-step process was followed to collect and develop this information. These steps included analyzing industry practices, conducting user interviews, distributing questionnaires, hosting a focus group meeting, and analyzing and documenting the information collected.

If your agency is considering purchasing encryption software, these reports may provide important information that can provide greater mission and agency efficiencies. The documents are located on the SAVER Web site (https://www.rkb.us/SAVER) as they become available. Reports on other technology being assessed in the SAVER Program can also be found on the Web site.